

34:2 BERKELEY TECHNOLOGY LAW JOURNAL

2019

Pages

343

to

704

Berkeley Technology Law Journal

Volume 34, Number 2

Production: Produced by members of the *Berkeley Technology Law Journal*.
All editing and layout done using Microsoft Word.

Printer: Joe Christensen, Inc., Lincoln, Nebraska.
Printed in the U.S.A.

The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Library Materials, ANSI Z39.48—1984.

Copyright © 2019 Regents of the University of California.
All Rights Reserved.



Berkeley Technology Law Journal
University of California
School of Law
3 Boalt Hall
Berkeley, California 94720-7200
btlj@law.berkeley.edu
<http://www.btlj.org>

BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 34

NUMBER 2

2019

TABLE OF CONTENTS

ARTICLES

AUTHORS AND MACHINES.....	343
<i>Jane C. Ginsburg & Luke Ali Budiardjo</i>	
LEGALLY COGNIZABLE MANIPULATION.....	449
<i>Ido Kivolaty</i>	
SECRECY & EVASION IN POLICE SURVEILLANCE TECHNOLOGY	503
<i>Jonathan Manes</i>	
UNCONSCIONABILITY 2.0 AND THE IP BOILERPLATE: A REVISED DOCTRINE OF UNCONSCIONABILITY FOR THE INFORMATION AGE.....	567
<i>Amit Elazari Bar On</i>	

SUBSCRIBER INFORMATION

The *Berkeley Technology Law Journal* (ISSN1086-3818), a continuation of the *High Technology Law Journal* effective Volume 11, is edited by the students of the University of California, Berkeley, School of Law and is published in print three times each year (March, September, December), with a fourth issue published online only (July), by the Regents of the University of California, Berkeley. Periodicals Postage Rate Paid at Berkeley, CA 94704-9998, and at additional mailing offices. POSTMASTER: Send address changes to Journal Publications, University of California, Berkeley Law—Library, LL123 Boalt Hall—South Addition, Berkeley, CA 94720-7210.

Correspondence. Address all correspondence regarding subscriptions, address changes, claims for non-receipt, single copies, advertising, and permission to reprint to Journal Publications, University of California, Berkeley Law—Library, LL123 Boalt Hall—South Addition, Berkeley, CA 94705-7210; (510) 643-6600; JournalPublications@law.berkeley.edu. *Authors:* see section titled Information for Authors.

Subscriptions. Annual subscriptions are \$65.00 for individuals and \$85.00 for organizations. Single issues are \$30.00. Please allow two months for receipt of the first issue. Payment may be made by check, international money order, or credit card (MasterCard/Visa). Domestic claims for non-receipt of issues should be made within 90 days of the month of publication; overseas claims should be made within 180 days. Thereafter, the regular back issue rate (\$30.00) will be charged for replacement. Overseas delivery is not guaranteed.

Form. The text and citations in the *Journal* conform generally to the THE CHICAGO MANUAL OF STYLE (16th ed. 2010) and to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 20th ed. 2015). Please cite this issue of the *Berkeley Technology Law Journal* as 34 BERKELEY TECH. L.J. ____ (2019).

BTLJ ONLINE

The full text and abstracts of many previously published *Berkeley Technology Law Journal* articles can be found at <http://www.btlj.org>. Our site also contains a cumulative index; general information about the *Journal*; the BTLJ Blog, a collection of short comments and updates about new developments in law and technology written by BTLJ members; and *BTLJ Commentaries*, an exclusively online publication for pieces that are especially time-sensitive and shorter than typical law review articles.

INFORMATION FOR AUTHORS

The Editorial Board of the *Berkeley Technology Law Journal* invites the submission of unsolicited manuscripts. Submissions may include previously unpublished articles, essays, book reviews, case notes, or comments concerning any aspect of the relationship between technology and the law. If any portion of a manuscript has been previously published, the author should so indicate.

Format. Submissions are accepted in electronic format through Scholastica online submission system. Authors should include a curriculum vitae and resume when submitting articles, including his or her full name, credentials, degrees earned, academic or professional affiliations, and citations to all previously published legal articles. The Scholastica submission website can be found at <https://scholasticahq.com/law-reviews>.

Citations. All citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 20th ed. 2015).

Copyrighted Material. If a manuscript contains any copyrighted table, chart, graph, illustration, photograph, or more than eight lines of text, the author must obtain written permission from the copyright holder for use of the material.

DONORS

The *Berkeley Technology Law Journal* and the Berkeley Center for Law & Technology acknowledge the following generous donors to Berkeley Law's Law and Technology Program:

Partners

COOLEY LLP

HOGAN LOVELLS

FENWICK & WEST LLP

ORRICK, HERRINGTON &
SUTCLIFFE LLP

WHITE & CASE LLP

Benefactors

BAKER BOTTS LLP

MORRISON & FOERSTER LLP

COVINGTON & BURLING LLP

POLSINELLI LLP

FISH & RICHARDSON P.C.

SIDLEY AUSTIN LLP

JONES DAY

WEIL, GOTSHAL & MANGES LLP

KIRKLAND & ELLIS LLP

WILMER CUTLER PICKERING HALE
AND DORR LLP

LATHAM & WATKINS LLP

WILSON SONSINI GOODRICH &
ROSATI

MCDERMOTT WILL & EMERY

WINSTON & STRAWN LLP

Corporate Benefactors

ATLASSIAN

LITINOMICS

COMPUTER & COMMUNICATIONS
INDUSTRY ASSOCIATION

MICROSOFT CORPORATION

CORNERSTONE RESEARCH

MOZILLA

FUTURE OF PRIVACY FORUM

NERA ECONOMIC CONSULTING

GOOGLE, INC.

NOKIA

HEWLETT FOUNDATION, THROUGH
THE CENTER FOR LONG-TERM
CYBERSECURITY

PALANTIR

INTEL

RLM TRIALGRAPHIX

INVENTIONSHARE

THE WALT DISNEY COMPANY

Members

BAKER & MCKENZIE LLP	KILPATRICK TOWNSEND & STOCKTON LLP
CROWELL & MORING	KNOBBE MARTENS LLP
DESMARAIS LLP	KWAN & OLYNICK LLP
DURIE TANGRI LLP	MORGAN, LEWIS & BOCKIUS LLP
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP	PAUL HASTINGS LLP
GTC LAW GROUP LLP & AFFILIATES	ROBINS KAPLAN LLP
HAYNES AND BOONE, LLP	ROPES & GRAY LLP
HICKMAN PALERMO BECKER BINGHAM	SIMPSON THACHER & BARTLETT LLP
IRELL & MANELLA LLP	TROUTMAN SANDERS LLP
KEKER VAN NEST & PETERS LLP	VAN PELT, YI & JAMES LLP
KILBURN & STRODE	WEAVER AUSTIN VILLENEUVE & SAMPSON LLP

BOARD OF EDITORS

2018–2019

Executive Board

Editor-in-Chief
ELLE XUEMENG WANG

Senior Articles Editors
LAURA KELLEY

Senior Executive Editor
ANGELA LYONS-JUSTUS

Managing Editor
CHRISTOPHER BROWN

ALEX BARATA
YARDEN KAKON

Senior Production Editor
MEGAN MCKNELLY

Senior Scholarship Editors
AMIT ELAZARI
NOMI CONWAY

Senior Annual Review Editors
CHRIS CHUANG
KATHARINE CUMMINGS

Senior Online Content Editor
KATHERINE BURKHART

Editorial Board

Submissions Editors
DANIEL CHASE
BEATRICE NYBERT

Production Editors
CHELSEY MORI
HAILEY YOOK
JANELLE LAMB
LOUISE DECOPPET

Technical Editors
MARIA BELTRAN
COLIN RAVELLE

Annual Review Editors
JULEA LIPIZ
AISLINN SMALLING

Notes & Comments Editors
NICK CALCATERRA
RYAN KWOCK

Symposium Editors
DARIUS DEHGHAN
JESSICA HOLLIS

Web Content Editors
CONCORD CHUNG
CHANTE ELIASZADEH

Podcast Editor
MIRANDA RUTHERFORD

LLM Editors
CRISTINA DE LA PAZ
MAYARA RUSKI
AUGUSTO SA

Member Relations Editor
CLARA CHOI

Alumni Relations Editor
NIR MAOZ

External Relations Editor
ANDREA SHEN

CHELSEA ANDRE
TIAGO AQUINO
SAVANNAH CARNES
ELSIE CHEANG
SHERILYN CHEW

Articles Editors
NITESH DARYANNANI
LESLIE DIAZ
GRACE FERNANDEZ
VESTA GOSHTASBI
ALEXANDER KROIS
NINA MILOSAVLJEVIC

CRISTINA MORA
COURTNEY REED
WESLEY TIU
MEI XUAN
LI ZHANG

MEMBERSHIP

Vol. 34 No. 2

Associate Editors

MADISON BOWER	YUAN FANG	ARYEH PRICE
MUHTADI CHOUDHURY	HARRISON GERON	MARTA STUDNICKA
MATTHEW CHUNG	ADRIAN KINSELLA	THERESA TAN
ELLA PADON CORREN	CLARA KNAPP	EMILEE WU
CHRISTINA CROWLEY	VICKY WEI-CHI LEE	CHENZHAO YU
DAVID FANG	HUI-FANG LIN	MICHELLE ZIPERSTEIN
	ALLAA MAGEID	

Members

GABRIELA ABREU	KERENSA GIMRE	ERIN MOORE
RIDDHI ADHIKARI	KELLY GO	WALTER MOSTOWY
SAFIYA AHMED	SARAH GOLD	LIU QING NG
MIMANSA AMBASTHA	ANDREW GORIN	YUTA OISHI
NISHANT ANURAG	KEVIN GU	BIHTER OZEDIRNE
ARTIN AU-YEUNG	PETER GUTMAN	VALINI PANTA
EMILY AVAZIAN	DEREK HA	SORA PARK
CHRISTOPHER BARCLAY	CATHERINE HARRIS	CHULHYUN PARK
VERONICA BOGNOT	DYLAN HELGESON	AYESHA RASHEED
ALEXIS CALIGIURI	ERIN HILLIARD	NOELLE REYES
ANNA ESCRIGAS	ALLAN HOLDER	BRYCE ROSENBOWER
CANAMERAS	JEONGHOON HONG	JOHN RUNKEL
LAUREN CARROLL	FIONA HUANG	RYAN JORGENSEN
CLAIRE CHANG	VICTORIA CONSTANCE HUANG	ARMBIEN SABILLO
ALEX CHEMEKINSKY	JONATHAN HUANG	GINETTA SAGAN
KEVIN CHEN	MAISIE IDE	TARINI SAHAI
TIFFANY CHEN	YING JIANG	SHREYA SANTHANAM
YITING CHENG	SAACHI JUNEJA	JOSH SEDGWICK
ARI CHIVUKULA	GIA JUNG	EVAN SEEDER
CLAIRE CHRISTENSEN	MARGARETH KANG	VICKY EL KHOURY SFEIR
SCOT CONNER	CHAITANYA KAUSHIK	YAAMINI SHARMA
JULIEN CROCKETT	JORGE KINA	CARMEN SOBCZAK
ARPITA DAS		
SAMAPIKA DASH		

TRENTON DAVIS	DANNY KONINGISOR	SCHUYLER STANDLEY
LIZ DOUGLASS	MICHAEL KOSTUKOVSKY	LYRIC STEPHENSON
IDA EBEID	KRISTINA KRASNIKOVA	DANIEL TODD
RUCHA EKBOTE	SOUMYA JOGAIHAH	VIVIANE TROJAN
KATELYN FELICIANO	KRISHNARAJU	DANIEL TWOMEY
OLGAMARIS	EMMA LEE	EDGAR VEGA
FERNANDEZ	JIAN LEE	YUHAN WANG
MORITZ FLECHSENHAR	KILLIAN LEFEVRE	GRACE WINSCHER
YESENIA FLORES	ELLY LEGGATT	JOLENE XIE
JASON FRANCIS	XIAOCAO LI	KEVIN YANG
LOGAN FREEBORN	ASHLEIGH LUSSENDEN	ALISON YARDLEY
RAVIN GALGOTIA	AARTIKA MANIKTALA	CLARK ZHANG
MARIBEL GARCIA	MARISSA MEDANSKY	JIEYU ZHANG
GARIMA GARG	ALEX MILNE	PENGPENG ZHANG
	ALEXANDRE MOCHON	EVAN ZIMMERMAN

BTLJ ADVISORY BOARD

JIM DEMPSEY
*Executive Director of the
Berkeley Center for Law & Technology*
U.C. Berkeley School of Law

ROBERT C. BERRING, JR.
*Walter Perry Johnson
Professor of Law, Emeritus*
U.C. Berkeley School of Law

MATTHEW D. POWERS
Tensegrity Law Group, LLP

JESSE H. CHOPER
Earl Warren Professor of Public Law
U.C. Berkeley School of Law

PAMELA SAMUELSON
*Professor of Law & Information
and Faculty Director of the
Berkeley Center for Law & Technology*
U.C. Berkeley School of Law

REGIS MCKENNA
Chairman and CEO
Regis McKenna, Inc.

LIONEL S. SOBEL
Visiting Professor of Law
U.C.L.A. School of Law

PETER S. MENELL
*Koret Professor of Law and Faculty
Director of the Berkeley Center
for Law & Technology*
U.C. Berkeley School of Law

LARRY W. SONSINI
Wilson Sonsini Goodrich & Rosati

ROBERT P. MERGES
*Wilson Sonsini Goodrich & Rosati Professor of
Law and Faculty
Director of the Berkeley Center
for Law & Technology*
U.C. Berkeley School of Law

MICHAEL STERN
Cooley LLP

DEIRDRE K. MULLIGAN
*Associate Professor and Faculty Director of the
Berkeley Center for
Law and Technology*
U.C. Berkeley School of Information

MICHAEL TRAYNOR
Cobalt LLP

JAMES POOLEY
James Pooley, PLC

THOMAS F. VILLENEUVE
Gunderson Dettmer Stough Villeneuve
Franklin & Hachigian LLP

BERKELEY CENTER FOR LAW & TECHNOLOGY 2018–2019

Executive Director

JIM DEMPSEY

Faculty Directors

KENNETH A. BAMBERGER	PETER S. MENELL	PAMELA SAMUELSON
CATHERINE CRUMP	ROBERT P. MERGES	PAUL SCHWARTZ
CATHERINE FISK	DEIRDRE K. MULLIGAN	ERIK STALLMAN
CHRIS HOOFNAGLE	TEJAS NARECHANIA	JENNIFER M. URBAN
SONIA KATYAL	ANDREA ROTH	MOLLY S. VAN HOUWELING

Fellow

KATHRYN HASHIMOTO

Staff Directors

JANN DUDLEY	IRYS SCHENKER
RICHARD FISK	MATTHEW RAY

AUTHORS AND MACHINES

Jane C. Ginsburg[†] & Luke Ali Budiardjo^{††}

ABSTRACT

Machines, by providing the means of mass production of works of authorship, engendered copyright law. Throughout history, the emergence of new technologies tested the concept of authorship, and courts in response endeavored to clarify copyright's foundational principles. Today, developments in computer science have created a new form of machine, the "artificially intelligent" (AI) system apparently endowed with "computational creativity." AI systems introduce challenging variations on the perennial question of what makes one an "author" in copyright law: Is the creator of a generative program automatically the author of the works her process begets, even if she cannot anticipate the contents of those works? Does the user of the program become the (or an) author of an output whose content the user has at least in part defined?

This Article frames these and similar questions that generative machines provoke as an opportunity to revisit the concept of copyright authorship in general and to illuminate its murkier corners. This Article examines several fundamental relationships (between author and amanuensis, between author and tool, and between author and co-author) as well as several authorship anomalies (including the problem of "accidental" or "indeterminate" authorship) to unearth the basic principles and latent ambiguities which have nourished debates over the meaning of the "author" in copyright. This Article presents an overarching and internally consistent model of authorship based on two basic pillars: a mental step (the conception of a work) and a physical step (the execution of a work), and defines the contours of these basic pillars to arrive at a cohesive definition of authorship.

The Article then applies the conception-and-execution theory of authorship to reach a series of conclusions about the question of machine "authorship." Even the most technologically advanced machines of our era are little more than faithful agents of the humans who design or use them. Asking whether a computer can be an author therefore is the "wrong" question; the "right" question addresses how to evaluate the authorial claims of the humans involved in either preparing or using the machines that "create." In many cases, either the upstream human being who programs and trains a machine to produce an output, or the downstream human being who requests the output, is sufficiently involved in the conception and execution of the resulting work to claim authorship. But in some instances, the contributions of the human designer and user will be too attenuated from the work's creation for either to qualify as "authors"—leaving the work "authorless."

DOI: <https://doi.org/10.15779/Z38SF2MC24>

© 2019 Jane C. Ginsburg & Luke Ali Budiardjo.

[†] Morton L. Janklow Professor of Literary and Artistic Property Law, Columbia Law School.

^{††} Columbia Law School JD Class of 2018. Many thanks to the members of the Columbia Law School faculty workshop; Ben Bogart, PhD; Madeline Rose Finkel; Rebecca Giblin and François Petitjean; Jeremy Kessler; Catherine Kessedjian; Ed Klaris; Enoch Liang and James Lee; Samuel Pitkin Niles; Javed Qadrud-Din; Blake Reese; and Jeffrey Stein.

TABLE OF CONTENTS

I.	INTRODUCTION	345
II.	BEFORE AI—CHALLENGES PRESENTED BY MECHANICAL AND NATURAL FORCES.....	352
A.	THE CONJOINED COMPONENTS OF AUTHORSHIP: DETAILED CONCEPTION + CONTROLLED EXECUTION	354
B.	AUTHORS AND AMANUENSES: THE PRINCIPAL-AGENT RELATIONSHIP	358
C.	WHEN RANDOM FORCES, FAUNAL OR METEOROLOGICAL, INTERVENE IN THE CREATIVE PROCESS.....	361
D.	THE LIMITS OF THE AUTHOR’S “CONCEPTION”	366
	1. <i>Curing Deficiencies in Conception: The “Adoption” Theory of Authorship.....</i>	366
	2. <i>Conception via Process</i>	370
E.	ALLOCATING AUTHORSHIP BETWEEN UPSTREAM AND DOWNSTREAM AUTHORS	374
F.	SHARING AUTHORSHIP: JOINT WORKS.....	378
	1. <i>Categories of Joint Works and Modes of Co-Authorship.....</i>	378
	2. <i>Contemporaneous “Intent to Merge” and Unacquainted Co- Authors</i>	381
	3. <i>Why Congress Required Contemporaneous Intent to Merge Contributions</i>	383
	a) Merger of Inseparable Contributions Without Collaboration?.....	387
	b) The Implications of Collaboration Between Co- Authors.....	389
III.	AUTHORSHIP OF COMPUTER-ENABLED OUTPUTS.....	392
A.	THE PROBLEM(?) OF ARTIFICIAL INTELLIGENCE	393
	1. <i>The Wrong Question: Machine “Authorship”</i>	393
	2. <i>Machine Learning and the “Black Box” Problem</i>	401
B.	THE RIGHT QUESTION: SEARCHING FOR THE HUMAN AUTHOR	404
	1. <i>“Ordinary” Tools: Those Whose Outputs Reflect the Creative Contributions of Their Users</i>	405
	2. <i>Fully-Generative Machines: Those Whose Outputs Reflect the Creative Contributions of Their Designers.....</i>	407
	3. <i>Partially-Generative Machines: Those Whose Outputs Reflect a Combination of the Creative Contributions of Designer and User.....</i>	413
C.	AUTHORSHIP AND PARTIALLY-GENERATIVE MACHINES	417

1.	<i>Distinguishing Between Fully- and Partially-Generative Machines: Can the Upstream Creator Claim Ownership of All Resulting Outputs?</i>	417
a)	Describing the Distinction.....	417
b)	Prior Judicial Approaches to This Question.....	419
c)	Approaches to the Distinction Between Fully and Partially Generative Machines.....	422
2.	<i>Dealing with Partially-Generative Machines: Who Executes the Work?</i>	426
IV.	THE AUTHORLESS OUTPUT	433
A.	WHAT COMPUTER-ENABLED WORKS ARE “AUTHORLESS”?	433
B.	REEXAMINING AUTHORSHIP DOCTRINE TO AVOID THE CLASSIFICATION OF MACHINE-ENABLED OUTPUTS AS “AUTHORLESS”	437
1.	<i>Joint Authorship</i>	440
2.	<i>Sole Authorship</i>	443
V.	CONCLUSION: IF NOT COPYRIGHT, THEN WHAT?	445

I. INTRODUCTION

Machines, by providing the means of mass reproduction of works of authorship, engendered copyright law.¹ Later, cameras—machines employed to create works, rather than merely to reproduce them—called into question copyright’s coverage of works whose human authorship those machines purportedly usurped.² The digital era exacerbates the anxiety of authorship, as “artificial intelligence” supposedly supplants human artists, writers, and composers in generating visual, literary, and musical outputs indistinguishable

1. See, e.g., Brad A. Greenberg, *Rethinking Technological Neutrality*, 100 MINN. L. REV. 1495, 1502 (2016) (“Modern copyright law’s existence can be traced to a transcendent technology: the movable-type printing press.”); Paul Edward Geller, *Copyright History and the Future: What’s Culture Got To Do With It?*, 47 J. COPYRIGHT SOC’Y 209, 215–19 (2000) (tracing history of copyright law beginning with the introduction of the printing press in 15th century Europe).

2. See *infra* Section II.A (discussing the debate about copyright in photographic works); see also Christine Haight Farley, *The Lingering Effects of Copyright’s Response to the Invention of Photography*, 65 U. PITT. L. REV. 385, 388 (2004) (noting that photography was the “first technological challenge” for copyright law).

from human-produced endeavors.³ Other commentators have posited adapting copyright law to the challenges of machine authorship;⁴ we ask the predicate questions: What is authorship in copyright law, and how do its precepts apply to machine-enabled outputs? In addressing the first question, and in keeping with the 1976 Copyright Act's general norm of technological neutrality,⁵ we derive general principles of authorship from copyright cases arising in the analog world in order to apply them to emerging modes of machine-implicated creativity. Only after ascertaining whether computer-enabled outputs are works of authorship according to underlying principles of copyright law can one determine whether, for authorless outputs, copyright law provides the right regulatory regime, or whether these outputs instead require some other form, if indeed any, of intellectual property protection.

In an earlier study, addressing authorship in the analog world, one of us concluded that authorship in copyright entwines conception and execution.⁶ Our analysis here further develops those two essential elements. By “conception” we mean more than envisioning the general ideas for a work; we mean elaborating a detailed creative plan for the work. Conception guides the work’s “execution,” the process through which the author⁷ converts the plan to concrete form. This basic process—through which conception informs execution—underlies all acts of authorship.

Because U.S. copyright law requires that original works of authorship be fixed in a tangible medium of expression,⁸ the author must embody her detailed ideas; conception alone (no matter how novel or imaginative) does

3. See Annemarie Bridy, *Coding Creativity: Copyright and the Artificially Intelligent Author*, 2012 STAN. TECH. L. REV. 5, 27 (2012) (noting that “AI authorship” may have placed the copyright system in a “digitally induced crisis”).

4. See, e.g., Robert C. Denicola, *Ex Machina: Copyright Protection for Computer-Generated Works*, 69 RUTGERS U. L. REV. 251, 284 (2016) (arguing that “users” should be recognized as the “authors and owners of computer-generated works” if they initiate the creation of computer-generated expression).

5. See *N.Y. Times Co. v. Tasini*, 533 U.S. 483, 502 (2001) (noting that the “transfer of a work between media does not ‘alter the character’ of that work for copyright purposes”); 4 MELVILLE B. NIMMER & DAVID NIMMER, *NIMMER ON COPYRIGHT* § 12A.16(b) (1963) (referring to technology neutrality as a “unifying theme” of the 1976 Act) [hereinafter *NIMMER ON COPYRIGHT* § 12A.16(b)].

6. Jane C. Ginsburg, *The Concept of Authorship in Comparative Copyright Law*, 52 DEPAUL L. REV. 1063, 1072 (2003) (“An ‘author’ conceives of the work and supervises or otherwise exercises control over its execution.”).

7. Or the author’s agents or collaborating co-authors; see *infra* Sections II.B and II.F, respectively.

8. 17 U.S.C. § 102(a) (2018).

not suffice to create a protectable work.⁹ But neither does mere execution; the amanuensis who transcribes an author's words, or the welder who follows the artist's instructions to create a monumental size rendition of the artist's model for a sculpture¹⁰ are not "authors" of the resulting works. Where the author directs another to give concrete form to the author's conception, and the person executing the assigned task acts within the intended scope of the author's delegation of authority, then the assistant's contribution lacks the "intellectual conception[]"¹¹ that characterizes an original work of authorship.¹²

Where, by contrast, the assistant participates in the conceptual elaboration, she may be a co-author, or even a sole author, when the instructions offer no more than a general idea and the assistant devises her own creative plan. St. Exupéry's *Little Prince* commanded the downed aviator: "Draw me a sheep!"¹³ The imperious little boy was not the author of the resulting image (a rather scrawny ovine). Had he instead detailed the sheep's intended appearance (for example, color, length, and curl of pelt; roundness of form; openness of eyes and mouth, etc.), he might have shared authorship with the aviator who gave visual form to the boy's words.¹⁴ But only if the aviator had made no personal expressive choices in his rendering of the "ideas in the mind"¹⁵ of the *Little*

9. *See* *Cnty. for Creative Non-Violence v. Reid*, 490 U.S. 730, 737 (1989) ("As a general rule, the author is the party who actually creates the work, that is, the person who translates an idea into a fixed, tangible expression entitled to copyright protection.").

10. For example, Alexander Calder has routinely relied on a metal-working shop to create his massive stabile sculptures. *See infra* notes 118–120 (discussing Calder's process of working with a team of welders).

11. *See* *Burrow-Giles Lithographic Co. v. Saroni*, 111 U.S. 53, 58 (1884) ("We entertain no doubt that the Constitution is broad enough to cover an act authorizing copyright of photographs, so far as they are representatives of original intellectual conceptions of the author.").

12. *See* *Andrien v. S. Ocean Cty. Chamber of Commerce*, 927 F.2d 132, 135 (3d Cir. 1991) ("[W]riters are entitled to copyright protection even if they do not perform with their own hands the mechanical tasks of putting the material into the form distributed to the public."); *see also* *Lindsay v. The Wrecked & Abandoned Vessel R.M.S. Titanic*, No. 97 Civ. 9248 (HB), 1999 WL 816163, at *4–6 (S.D.N.Y. Oct. 13, 1999) (affirming the authorship claim of the director of a documentary film about the *R.M.S. Titanic* who had "exercised . . . a high degree of control over a film operation," and was the "driving force behind the final film product," and dismissing defendants' objection that the director "[could] not have any protectable right in the . . . footage since he did not dive to the ship and thus did not himself actually photograph the wreckage").

13. *See* ANTOINE DE ST. EXUPÉRY, *THE LITTLE PRINCE* 9 (1943).

14. *Cnty. for Creative Non-Violence*, 490 U.S. at 753 (indicating, but not deciding, that the commissioning party might give such detailed instructions as to become a co-author).

15. *Burrow-Giles*, 111 U.S. at 58 (noting that the scope of copyright includes "all forms of writing, printing . . . etc., by which the ideas in the mind of the author are given visible expression").

Prince (an unlikely prospect given the hand-drawn medium),¹⁶ would the Little Prince have been a sole author.

While these copyright precepts are well-settled, challenges arise when the putative author partners with a machine or with natural forces to create a work of authorship. These paired productions require us to ask whether they are “original works of authorship” entitled to copyright protection. The burgeoning of computer-enabled works¹⁷—outputs of generative machines¹⁸ designed to create works and to mimic human creativity, perhaps through the use of “artificial intelligence”¹⁹ techniques like machine learning—offers the newest iteration of those challenges. But the questions AI raises precede the

16. *Bleistein v. Donaldson Lithographing Co.*, 188 U.S. 239, 250 (1903) (“Personality always contains something unique. It expresses its singularity even in handwriting, and a very modest grade of art has in it something irreducible, which is one man’s alone. That something he may copyright unless there is a restriction in the words of the act.”).

17. This Article uses the term “computer-enabled” or “machine-enabled” and avoids the more commonly used term “computer-generated” to highlight that the machines themselves do not necessarily *generate* or *author* these works—but that instead humans produce the works with the *assistance* of sophisticated generative machines. See *infra* Section III.A (rejecting the idea of “machine authorship” and instead arguing that machines should be considered tools of their creators).

18. “Generative machine” refers to any machine, other than a mere “ordinary tool,” that “contributes to or results in a completed work,” either by creating a work at the push of a button (“fully-generative” machines) or by inviting the user to input instructions, which guide and inform a creative output, thereby fusing the creative contributions of the machine’s designer and user (“partially-generative” machines). See Philip Galanter, *Thoughts on Computational Creativity*, DAGSTUHL SEMINAR PROCEEDINGS 09291 - COMPUTATIONAL CREATIVITY: AN INTERDISCIPLINARY APPROACH (2009), <http://drops.dagstuhl.de/opus/volltexte/2009/2193/> [<https://perma.cc/D5MQ-JCW2>] (introducing the definition and theories of generative machines); *infra* Section III.B.1 (discussing “ordinary tools”); *infra* Sections III.B.2–3 (discussing and defining “fully-generative” and “partially-generative” machines).

“Generative machine” also includes “generative models.” See, e.g., Andrej Karpathy et al., *Generative Models*, OPENAI BLOG (June 16, 2016), <https://blog.openai.com/generative-models/> [perma.cc/9LX9-9Q6F] (“To train a generative model we first collect a large amount of data in some domain (e.g., think millions of images, sentences, or sounds, etc.) and then train a model to generate data like it.”). However, “generative machine” also includes machines and systems built for the purpose of creating “generative art.” See Galanter, *supra* note 18 (providing a “wide” definition of the term “generative art” which refers to “any art practice where the artist cedes control to a system that . . . contributes to or results in a completed work of art”).

19. The term “artificial intelligence” is an “umbrella term,” comprising “many different techniques,” and broadly refers to the “set of techniques aimed at approximating some aspect of human or animal cognition using machines.” Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 404–05 (2017).

digital era.²⁰ These questions arose with the advent of photography and persist whenever a work's creator incorporates uncontrolled forces, whether faunal or meteorological, mechanical or digital, to generate the work.

Part II of this Article reviews non-digital examples to derive general principles of copyright authorship. All non-digital examples present an intervening element complicating the putative author's causal relationship to the creation of the work. Thus, in addition to mechanical and natural forces, this Article considers whether the participation of another human contributor deprives the initiator of sole or even any claim to authorship.

Part III applies those traditional principles to explore the authorship status of potential computer-enabled outputs. Properly programmed computers may increasingly encroach on human execution of a work, but their role in engendering the work's conception is far more debatable. Because computers today, and for proximate tomorrows, cannot themselves formulate creative plans or "conceptions" to inform their execution of expressive works, they lack the initiative that characterizes human authorship.²¹ The computer scientist who succeeds at the task of "reduc[ing] [creativity] to logic" does not generate new "machine" creativity²²—she instead builds a set of instructions to codify and simulate "substantive aspect[s] of human [creative] genius," and then commands a computer to faithfully follow those instructions.²³ Even the most sophisticated generative machines proceed through processes designed entirely by the humans who program them, and are therefore closer to amanuenses than to true "authors."²⁴ Therefore, even if the concept of

20. See Benjamin L.W. Sobel, *Artificial Intelligence's Fair Use Crisis*, 41 COLUM. J.L. & ARTS 45, 47 (2017) (noting that the question "Can a computer be an author?" is "not as novel as it may seem" and noting that "[o]ver a century has passed since the Supreme Court first evaluated whether the outputs of a new creative technology, capable of operating with less human oversight than its predecessors, could manifest authorship to the degree intellectual property laws required . . . [t]hat technology was photography").

21. See *infra* Section III.A.1 (discussing and rejecting the possibility of true "machine authorship").

22. SELMER BRINGSJORD & DAVID FERRUCCI, *ARTIFICIAL INTELLIGENCE AND LITERARY CREATIVITY: INSIDE THE MIND OF BRUTUS, A STORYTELLING MACHINE* xiii, xvi (1999) (describing the task of generating a machine capable of writing fiction as the "attempt to reduce creativity to computation").

23. *Id.* at xxii, xxiv ("As we uncover reasons for believing that human creativity is in fact beyond the reach of computation, we will be inspired to nonetheless engineer systems that dodge these reasons and *appear* to be creative.").

24. Cf. Jack M. Balkin, *2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1223–24 (2018) (describing the "homunculus fallacy," or the "way that people tend to think about robots, AI agents, and algorithms" with the "belief that there is a little person inside the program who is

“author” in the U.S. Constitution and the Copyright Act could encompass non-human actors,²⁵ the machines of today would not qualify as “authors.” Asking whether a computer can be an author therefore is not a fruitful inquiry.

Having dismissed computer authorship as the “wrong” question, this Article focuses instead on the “right” question: how to evaluate the authorial claims of the humans involved in either preparing or using the machines that “create.” Thus, in Part III, this Article ascertains whether the upstream human being who programs and trains a computer to produce an output, or the downstream human being who requests the output, is the (or an) author of the resulting production based on authorship principles. In other words, Part III probes the distinction between a “tool” (output attributable to the user) and a

making it work,” and arguing that “[w]hen we criticize algorithms, we are really criticizing the programming, or the data, or their interaction. But equally important, we are also criticizing the use to which they are being put by the humans who programmed the algorithms, collected the data, or employed the algorithms and the data to perform particular tasks”); Carys Craig & Ian Kerr, *The Death of the AI Author* 25 (Osgoode Legal Studies Research Paper, 2019) (“It is important to remember . . . that[] even if a machine predicts all the right words . . . it neither knows, understands, nor appreciates the connotation of its word assemblage, let alone the meaning or value of the ‘work’ as a whole.”).

25. Many authorities concur that “authorship” in copyright law implies human creativity. *See* *Naruto v. Slater*, 888 F.3d 418, 426 (9th Cir. 2018) (holding that “animals other than humans . . . lack statutory standing to sue under the Copyright Act”); *see also* *Urantia Found. v. Maaherra*, 114 F.3d 955, 958 (9th Cir. 1997) (“For copyright purposes, however, a work is copyrightable if copyrightability is claimed by the first *human beings* who compiled, selected, coordinated, and arranged [the work].”) (emphasis added); UNITED STATES COPYRIGHT OFFICE, COPYRIGHT OFFICE PRACTICES COMPENDIUM §§ 306, 313.2 (2017) [hereinafter COMPENDIUM] (noting that “the Office will refuse to register a claim if it determines that a human being did not create the work” and “the Office will not register works produced by a machine or mere mechanical process that operates randomly or automatically without any creative input or intervention from a human author”). *But see* Denicola, *supra* note 4, at 265–69 (raising doubt about the existence of a human-authorship requirement); Arthur R. Miller, *Copyright Protection for Computer Programs, Databases, and Computer-Generated Works: Is Anything New Since CONTU?*, 106 HARV. L. REV. 977, 1060–65 (1993) (concluding that “[i]t is far from clear that the federal courts ultimately will conclude that our copyright law requires human authorship,” and that “[t]he Constitution[] . . . does not mandate that authors be flesh and blood”). For a recent exploration of the human authorship requirement in the context of artificially-intelligent machines, see generally Craig & Kerr, *supra* note 24, at 41–42 (“[T]he outputs generated by AI—whether or not that AI passes a Turing test—are never in fact ‘the same’ as the human creations they seek to imitate. . . . If text is a vehicle through which our consciousness relates to another consciousness—one or any, immediate or asynchronous—then authorship presupposes something that AI does not have, and cannot produce. . . . To say authorship is human, that it is fundamentally connected with humanness . . . is to say that human communication is the very point of authorship as a social practice, indeed as a condition of life.”).

truly “generative” machine (output attributable to the programmer of the machine).

Part IV shows that the answer may often be “neither,” even when these authorless outputs’ literary, musical, or artistic *appearance* would surely soar over the minimal threshold of creativity required of traditionally-authored works. Nonetheless their lack of an author—i.e., a creative actor who both conceives of and executes the work—would disqualify them from copyright subject matter. If divergent treatment of otherwise potentially identical human-generated and authorless machine-enabled works seems problematic, it may be appropriate to revisit some of the analog world principles whose application may render many computer-enabled outputs “authorless.” Current doctrines of joint works, or distinguishing ideas from expression, furnish likely candidates for revision. The former reform would pair the downstream user with the upstream programmer(s) as co-authors. The latter would permit the designation of the downstream task-assigner as the “author,” a solution the UK and other Commonwealth countries have adopted.²⁶ Nonetheless, the reluctance to strand computer-enabled outputs on authorless shores does not warrant relaxing the statutory and the case law criteria in either instance, notably because accommodations for the inclusion into copyright of otherwise authorless outputs are unlikely to remain cabined to that context.²⁷

This Article concludes this exploration of copyright authorship with a taxonomy of outputs, from those enjoying copyright protection by virtue of their human-dominated creation to those lacking sufficient human participation to characterize the output as an “original work of authorship.” As to the latter group, some may fear that a complete lack of protection for authorless outputs might discourage the development of the technologies or of the business models required to produce and commercialize these outputs. But one should not simply assume that without copyright-like protection,

26. *See, e.g.*, Copyright, Designs and Patents Act 1988, c. 48, § 178(b) (U.K.) (defining a “computer-generated” work as a work “generated by computer in circumstances such that there is no human author of the work”); *see also id.* at § 9(3) (“In the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken.”); Copyright Ordinance, (1997) Cap. 528, § 11(3) (H.K.) (same); Copyright and Related Rights Act 2000 (Act No. 28/2000) § 21(f) (Ir.) (same); Copyright Act 1994, s 5, sub 2, pt a (N.Z.) (same); Copyright Act 98 of 1978 § 1 (S. Afr.) (same); *cf.* Copyright Act, 1957, No. 14, Acts of Parliament, 1957 § 2(d)(vi) (India) (“‘Author’ means . . . in relation to . . . [a] work which is computer-generated, the person who causes the work to be created.”).

27. *See* Kalin Hristov, *Artificial Intelligence and the Copyright Dilemma*, 57 IDEA 431, 441 (2017) (“Redefining copyright authorship to include non-human authors would undermine the current U.S. legal system, creating further uncertainty by raising more questions than answers.”).

society will be deprived of these benefits. Any regime design must ascertain the kinds of incentives (if any) different sorts of authorless outputs might require. To the extent that proponents of protection can empirically demonstrate the necessity for some form of coverage, regime design must also consider how to tailor the impetus to the need.

II. BEFORE AI—CHALLENGES PRESENTED BY MECHANICAL AND NATURAL FORCES

This Part identifies conception and execution as the hallmarks of authorship and examines the emergence of their articulation in the progression of U.S. copyright cases elaborating these two terms. Section II.A discusses conception and execution in controversies involving photography—the first cases of alleged “machine authorship.” If the process of authorship consists of the “conversion of . . . ‘things of the mind into transferable articles of property,’”²⁸ this transformation implies two predicate steps: first, a creative plan, and, second, the physical generation of a tangible “work” executing that plan. The “core concept” of authorship, therefore, is “creativity in *conceiving* the work and controlling its *execution*.”²⁹

Section II.B then considers scenarios that validate the claims of the initiator of a work of authorship, in cases involving amanuenses—participants we cast as “agents” of the author-principal. Sections II.A and II.B together demonstrate that the law does not require that to “execute” the work, the author have by her own hand given physical form to its every element. Section II.C shifts to scenarios that challenge the initiator’s authorship status, in instances involving the intervention of uncontrolled external natural or random causal forces in the execution of the work.

Section II.D assesses the extent to which those instances might require more nuance when identifying authorship along the axes of conception and controlled execution. It reexamines the “conception” requirement, concluding that the author’s intellectual conception of the work need not reflect a complete or even an accurate prediction of the resulting work’s contents. Copyright case law encompasses works that result from acts of unintended or accidental creativity,³⁰ despite the dissonance between what the author

28. ALVIN KERNAN, *THE DEATH OF LITERATURE* 123 (1990) (quoting Sutherland, in *Plagiarism—A Symposium*, *Times* (London) *Literary Supp.*, Apr. 9, 1982, at 414, col. 4).

29. Ginsburg, *supra* note 6, at 1067, 1072 (“An ‘author’ conceives of the work and supervises or otherwise exercises control over its execution.”).

30. *See id.* at 1086 (noting that “images generated by bad eyesight, claps of thunder, and frustrated flinging of sponges” are protected by copyright); *see, e.g.*, SUSAN SONTAG, *ON*

expected and how the final work turned out. “Accidental authorship” in fact merely presents an evocative example of the creative process: an author may create a work without precise foresight of the work’s ultimate form or contents. Acknowledging that conception may often be subsumed in contemporaneous execution, because the author’s conception of the work may emerge as she creates it, does not detract from conception’s cornerstone role in the process of authorship.

In effect, authorship’s “conception” element merely requires the author to devise a *creative plan* for the work. Accordingly, an author who is entirely responsible for formulating the work’s creative plan and executing that plan is presumptively the author of the resulting work. In most cases, there is no need to extricate these elements from the creative bundle. Scholars generally do not endeavor to ascertain whether the putative author in fact envisioned or how she brought forth the work. But we do call authorship into question if the circumstances of a work’s creation cast doubt on the attribution of authorship. As Section II.C discusses, natural or mechanical forces, if unmastered by a human being, may usurp the dominant role in a work’s execution, thus calling on courts to ascertain the actor to whom (or to which) to attribute the work’s creation.

Section II.E further discusses how the relationship among multiple (or competing) contributors to a work furnishes another basis for querying the creative process. When we inquire whether an amanuensis—an agent—has faithfully carried out her subordinate task (in which case she is not an author), or has instead struck out on her own creative path, we are asking whether she has wholly or partly superseded the principal’s authorship by furnishing her own “creative plan,” or by completing the insufficient creative plan supplied by the putative author.³¹ Similarly, when co-authorship aspirants claim to share authorship status, this Section investigates the extent of their alleged collaboration with the putative author, and the nature of the contributions they bring to the work.³²

PHOTOGRAPHY 117 (1977) (“[M]ost photographers have always had—with good reason—an almost superstitious confidence in the lucky accident.”); *see also* *Time Inc. v. Bernard Geis Assocs.*, 293 F. Supp. 130, 131 (S.D.N.Y. 1968) (Abraham Zapruder intended to film the presidential motorcade; he captured the JFK assassination “by sheer happenstance”); *infra* Section II.D.2.

31. The principal-agent dynamic offers another reason for declining to characterize computers as “authors”: agents violate the relationship by exceeding the scope of their delegated authority; a computer cannot (at least not now) go off on a “frolic of its own.” *See infra* Section III.A (discussing machines as “agents”).

32. *See infra* Sections II.E and II.F.

Accordingly, we consider the application of authorship's essential elements to the problem of works that inseparably merge the inputs of their various contributors. Section II.E provides a taxonomy of different relationships in situations involving multiple contributors to a single work and provides a framework to determine the allocation of sole authorship between "upstream" and "downstream" contributors.

Section II.F addresses the statutory criteria for joint works and co-authorship, and distinguishes works comprised of interdependent contributions from those whose components are inseparable. Part II concludes by demonstrating that if multiple creators contribute to the creation of a work but do not meet the statutory requirements of inseparable joint works, the resulting work may be "authorless."

A. THE CONJOINED COMPONENTS OF AUTHORSHIP: DETAILED
CONCEPTION + CONTROLLED EXECUTION

The advent of photography confronted judges with a novel task: to determine whether a human could claim authorship of a machine-generated image.³³ Prior mechanical adjuncts, from engraving through lithography, served as modes of reproduction of a pre-existing hand-drawn image. By contrast, without the camera's intervention, there would be no image. And while the photographer's manipulation of the camera or the subject might emulate the aesthetics of works directly formed by an artist's hand,³⁴ the camera substituted for the artist's hand in the initial fixation of the subject. This particularity in the means of creation sparked debate over the attribution of the output of the mechanical process. On the one hand, if the output owes its origin to a machine, then it lacks a human author, and by that token, cannot be the object of copyright. On the other hand, if the machine provides a means of expressing the photographer's vision of the image, and the author controls that means, then the machine has not displaced the author.

In 1879, Eugène Pouillet's *Traité pratique de la propriété littéraire et artistique* stated the cases for and against recognizing photographs as works of

33. See Farley, *supra* note 2, at 387–88 (describing the "invention of photography" as a "critical episode in the development of the authorship doctrine," and noting that the law "finds authorship in photographs" and "does not credit the technology as playing a role in the authorship").

34. *Id.* at 390 (noting ways "in which a photographer can manipulate the image" produced by a camera, and noting that "[t]hese activities . . . [have] definite analogies in the world of artistic production").

authorship.³⁵ Both sides shared the essential terms of the debate: does the output reflect the author's mental labor in the execution of the image? Articulating the case against authorship of a photograph, Pouillet distinguished "the labor of thought previous to execution" from "the mental labor in the material output."³⁶ Under this view, the law "does not protect the thought without the execution. . . . All of the intellectual and artistic work of the photographer is anterior to the material execution, his mind or his genius have nothing to do with this execution."³⁷ Painting and engraving are different, this side of the debate urges, because the law intervenes at the moment of materialization of the artist's conception, when he puts brush to canvas; the law does not afford protection to the artist's imagination before it assumes material form. By contrast, "the photographer erects his apparatus, he thenceforth remains a complete stranger to what is taking place; light does its work: a splendid but independent agent has accomplished all."³⁸

Shifting to the case in favor of copyright in photographs (a conclusion he endorsed), Pouillet disputed the disappearance of the author from the process of materializing his conception:

[I]t is always the thought of the artist which directs the instrument,—which guides and inspires the material means. Thought retains its supreme role. In photography, the apparatus takes the place, though not entirely, of hand labor,—the material part of the labor,—but it leaves to the artist, to its fullest extent, the labor of the mind. . . . The photographer conceives his work, he arranges the accessories and play of light, he arranges the distance of his instrument according as he wants, in the reproduction, either distinctness or size; thus, also, he obtains this or that effect of perspective.³⁹

Thus, from the outset, the analysis focused on the role of the human author not only in imagining what the work would look like, but in controlling the process of its materialization. Early photography cases in England and the United States tested both elements of the equation. In *Nottage v. Jackson*,⁴⁰ the dispute focused not on whether a photograph was a work of authorship, but

35. *Sarony v. Burrow-Giles Lithographic Co.*, 17 F. 591, 597–601 (1883) (quoting EUGÈNE POUILLET, *Property in Photographs*, in *TRAITÉ PRATIQUE DE LA PROPRIÉTÉ LITTÉRAIRE ET ARTISTIQUE* (William Alexandre Heydecker trans.) [hereinafter Pouillet on Photography]).

36. *Id.*

37. *Id.*

38. *Id.* at 597–98.

39. *Id.* at 599–601.

40. *Nottage v. Jackson* [1883] 11 QBD 627.

on who its author was. The claimants' employee had instructed a hired photographer to take the picture of an Australian cricketer.⁴¹ The Court of Queen's Bench upheld the challenge to the claimants' authorship: their role entailed neither a specific conception of the work nor any involvement in its execution. Lord Justice Cotton opined:

It is not the person who suggests the idea, but the person who makes the painting or drawing, who is the author. . . . [H]e must be the originator in the making of the painting or drawing. . . . The mere preparing the materials, or preparing and supplying of the instruments . . . cannot, in my opinion, make a man the author In my opinion, "author" involves originating, making, producing, as the inventive or master mind, the thing which is to be protected, whether it be a drawing, or a painting, or a photograph.⁴²

Lord Justice Bowen agreed:

I think it is evidently not the man who pays—not the man who contributes the machinery—not *the man who does nothing except form the idea*—not *the man who does nothing toward embodying the idea*—not the man who finances the expedition or who sends it out—none of those persons, in the ordinary sense of the term, can be considered the artist.⁴³

Thus, supplying the material or financial means to create a work does not make one its author. A work's "originator" does more than order its creation: she must both form and embody her concept for the work.⁴⁴

The U.S. Supreme Court applied the *Nottage* framework in a case decided the next year, but this time challenging whether a photograph, given the role of a machine in its creation, could be the "writing" of an "author." In *Burrow-Giles*,⁴⁵ the defendant had made lithographic copies of one of celebrity photographer Napoleon Sarony's portraits of Oscar Wilde. Construing those terms in the Constitutional copyright clause, the Supreme Court declared:

An author . . . is "he to whom anything owes its origin; originator; maker; one who completes a work of science or literature." . . . By writings in that clause is meant the literary productions of those authors, and Congress very properly has declared these to include all

41. *Id.* at 630.

42. *Id.* at 634–35.

43. *Id.* at 636 (emphasis added).

44. *See* Ginsburg, *supra* note 6.

45. *Burrow-Giles Lithographic Co. v. Sarony*, 111 U.S. 53 (1884).

forms of writing, printing, engraving, etching, etc., by which the ideas in the mind of the author are given visible expression.⁴⁶

The “writing” thus embodies the “author’s” conception of the work, but the Court’s description indicates that authorship requires more than a disembodied idea of the work. If the “author” is the “maker” or “one who completes a work of science or literature,”⁴⁷ then authorship conjoins conception and execution. The defendant nonetheless urged that the mechanical and chemical operations of the photographic process, designed to produce the most accurate representation of “some existing object,” precluded any “intellectual conception” on Sarony’s part.⁴⁸ Whether or not such lack of creativity might “be true in regard to the ordinary production of a photograph,”⁴⁹ the Court abstained from generalizing, approvingly citing the lower court’s finding that Sarony made his photograph

entirely from his own original mental conception, to which he gave visible form by posing the [subject] in front of the camera, selecting and arranging the costume, draperies, and other various accessories in said photograph, arranging the subject so as to present graceful outlines, arranging and disposing the light and shade, suggesting and evoking the desired expression, and from such disposition, arrangement, or representation, made entirely by plaintiff, he produced the picture in suit.⁵⁰

Although Oscar Wilde did not “owe[] [his] origin” to Napoleon Sarony, the photographer created the *mise en scène* depicting Wilde.⁵¹ Sarony did not, it appears, in fact press the camera’s shutter nor choose the precise moment to fix the image.⁵² Nonetheless, Sarony’s selection and arrangement of the component visual elements “gave visible form” to his “own original mental conception.”⁵³ The Supreme Court’s decision thus points to two precepts. First, a machine does not usurp authorship when it fixes a carefully composed

46. *Id.* at 57–58.

47. *Id.*; see also *Cnty. for Creative Non-Violence v. Reid*, 490 U.S. 730, 737 (1989) (“As a general rule, the author is the party who actually creates the work, that is, the person who translates an idea into a *fixed, tangible expression* entitled to copyright protection.”) (emphasis added); *Sands & McDougall Proprietary Ltd. v. Robinson* [1917] HCA 14; (1917) 23 CLR 55 (Isaacs, J.) (Austl.) (“[I]n copyright law the two expressions ‘author’ and ‘original work’ have always been correlative; the one connotes the other.”).

48. *Burron-Giles*, 111 U.S. at 59.

49. *Id.*

50. *Id.* at 60.

51. See *id.* at 58.

52. See Farley, *supra* note 2, at 434–35 (noting the role of Sarony’s cameraman).

53. *Burron-Giles*, 111 U.S. at 60.

image. The mechanical and chemical processes may capture reality, but the author has constructed the arrangement of the “existing object[s]” and their lighting to express her intellectual conception of the image.⁵⁴ Second, the author may delegate the physical embodiment of her conception, that is, the execution of the work, to an assistant, yet still retain authorship, at least where the execution hews closely to the author’s conception. The Supreme Court cited the Justices of the Queen’s Bench in *Nottage v. Jackson* at length, including Lord Justice Cotton’s evocation of the author as the “master mind” of the photographic image, and the Master of the Rolls’ statement that the author is “the person who has superintended the arrangement, who has actually formed the picture by putting the persons in position, and arranging the place where the people are to be.”⁵⁵ Sarony “actually formed the picture,” even though his assistant fixed the formation in the photographic plate.⁵⁶ The assistant was effectively an amanuensis whose creative contributions, if any, neither the Supreme Court nor the court below even considered.

B. AUTHORS AND AMANUENSES: THE PRINCIPAL-AGENT
RELATIONSHIP

Copyright law indeed distinguishes authors from amanuenses: as the late Justice Laddie of the High Court of England and Wales colorfully put it: “In my view, to have regard merely to who pushed the pen is too narrow a view of authorship. . . . It is wrong to think that only the person who carries out the mechanical act of fixation is an author.”⁵⁷ Rather, the law attributes authorship to the “mastermind,” whose detailed conception so controls its subsequent execution that the individuals carrying out the embodiment exercise no creative autonomy.⁵⁸ Attribution of authorship effectively follows general rules of agency: “the physical acts of the agent are attributed wholly to the author” under whose control and direction the amanuensis acts.⁵⁹

54. *Id.* at 59.

55. *Id.* at 61.

56. *Id.*

57. *Cala Homes v. Alfred McAlpine Homes* [1995] EWHC 7 (Ch).

58. *Burrow-Giles*, 111 U.S. at 61 (noting that the “author” is the “inventive or master mind” behind the work).

59. See RESTATEMENT (THIRD) OF AGENCY § 2.02(1) (AM. LAW INST. 2006) (“An agent has actual authority to take action designated or implied in the principal’s manifestations to the agent and acts necessary or incidental to achieving the principal’s objectives.”). The specific rules of agency law do not supply an exact parallel to author-amanuensis doctrine, but instead provide a structural parallel through which copyright law might deal with and rationalize the (often silent) role of the amanuensis. See, e.g., Elizabeth Adeney, *Authorship and Fixation in Copyright Law: A Comparative Comment*, 35 MELB. U. L. REV. 677 (2011) (noting that “when

The principal author “controls” the amanuensis when the principal author influences not only *what* the amanuensis does, but *how* she accomplishes her task. For example, in *Andrien v. South Ocean County Chamber of Commerce*,⁶⁰ the Third Circuit upheld the claimant’s sole authorship of a seaside community map whose contents he had extensively described to the defendant printer, even though the plaintiff did not in fact draw the map’s contours.⁶¹ The plaintiff did, however, closely supervise the printer’s execution of his instructions. The Third Circuit held that Andrien was the author of the work because Andrien had “directed the copy’s preparation in specific detail,” and because “[h]is compilation needed only simple transcription to achieve final tangible form,” the printer “acted as his amanuensis just as does a stenographer in typing material dictated by another person.”⁶² Like a faithful agent, the printer carried out its tasks as instructed, injecting no alterations of its own. And Andrien, as the principal author, utilized his control to influence and supervise the work’s execution: he dictated *how* the printer should make the work.

Similarly, in *Lindsay v. The Wrecked and Abandoned Vessel R.M.S. Titanic*,⁶³ the court attributed authorship to the film director who had extensively planned and controlled each shot, rather than to the underwater camera operators who actually filmed the sunken vessel:

All else being equal, where a plaintiff alleges that he exercised such a high degree of control over a film operation—including the type and amount of lighting used, the specific camera angles to be employed, and other detail-intensive artistic elements of a film—such that the final product duplicates his conceptions and visions of what the film should look like, the plaintiff may be said to be an ‘author’ within the meaning of the Copyright Act.⁶⁴

another person acts as an amanuensis to the author, the author will achieve copyright protection for the words recorded,” and that “[t]he physical acts of the agent or scribe are attributed wholly to the author who has supplied the words to be recorded”).

60. *Andrien v. S. Ocean Cty. Chamber of Commerce*, 927 F.2d 132 (3d Cir. 1991).

61. *Id.* at 133.

62. *Id.* at 135; *see also* WALTER ARTHUR COPINGER, *THE LAW OF COPYRIGHT* 109–10 (Stevens & Haynes, eds. 1915) (describing the case of *Stannard v. Harrison*, 1871 W.R. 811 (Eng.), in which the court held that the plaintiff who “cannot draw himself” and had thus employed another man to “make a [map] for him” was the author because he “invent[ed] the subject of the design beyond all question”).

63. *Lindsay v. Wrecked and Abandoned Vessel R.M.S. Titanic*, No. 97 Civ. 9248 (HB), 1999 WL 816163 (S.D.N.Y. Oct. 13, 1999).

64. *Id.* at *5 (noting further that “[t]he fact that Lindsay did not literally perform the filming,” and had not “[dove] to the wreck and operat[ed] the cameras, will not defeat his

Where, by contrast, the putative author's conception of the work does not fully constrain another's execution, or where the putative author exercises too little influence over *how* the other creator creates the work, the latter will be an author in her own right, because she will have exercised creative autonomy in her embodiment of the former's ideas. In giving concrete form to the work, she will have implemented her own ideas about the intended result. Indeed, the less formed the initial ideas and the less influence the putative principal author exercises over the process of execution, the less likely will sole, or even any, authorship be attributed to the person claiming to have conceived the work.⁶⁵

For example, in *Geshwind v. Garrick*,⁶⁶ the plaintiff Geshwind, a producer of computer graphics animation, worked with Leich, a third party's employee animator, to create a fifteen-second animated sequence simulating a flight over Japan. Geshwind supplied a topographical map and other information, but the animator, "acting entirely without Geshwind,"⁶⁷ created the sequence. Geshwind retained the right of approval, reviewed the sequence, and made suggestions that the animator did not always adopt. Although Geshwind asserted that he "gave Leich minute instructions in every aspect of [the work], to such an extent that it was his sole creation," the court credited the animator's account.⁶⁸ While Geshwind may have attempted to influence Leich's execution of the work,⁶⁹ his inability to influence Leich meant that he could not

claims of having 'authored' the . . . footage" because of the plaintiff's significant involvement in the film's pre- and post-production efforts).

65. See *Sheldon v. Metrokane*, [2004] 135 FCR 34, ¶ 85 (Austl.) (concluding that the respondent's agent, who had to a "limited extent" supervised the production and design of a corkscrew by a factory in China, was not the sole author of the resulting design "because of the input of unidentified persons . . . involved in the manufacturing and associated activities of the factory," and further noting that "the notion of authorship . . . is not satisfied merely by the giving of instructions to a manufacturer"). For a discussion of co-authorship, see *infra* Section II.F.

66. *Geshwind v. Garrick*, 734 F. Supp. 644 (S.D.N.Y. 1990).

67. *Id.* at 649.

68. *Id.* at 650.

69. *Id.* (noting that Geshwind may have "wanted changes in details and aspects of the [work] and even made suggestions"); see also F. Jay Dougherty, *Not A Spike Lee Joint? Issues in the Authorship of Motion Pictures Under U.S. Copyright Law*, 49 UCLA L. REV. 225, 244–45 (2001) (discussing the Geshwind case and noting that "[s]imply having the right to accept or reject expression originated by another, although a relevant factor in determining economic authorship, does not otherwise constitute authorship").

successfully claim that Leich was his creative agent; thus Leich's actions were those of an independent and sole author.⁷⁰

The amanuensis doctrine and the photography cases share a bottom line: the author (acting as principal) can outsource acts of execution to agents (machines or human helpers); as long as those agents act within the scope of the author's intended delegation of authority, and as long as the principal constrains how the agent carries out her task, the principal remains the author.

C. WHEN RANDOM FORCES, FAUNAL OR METEOROLOGICAL,
INTERVENE IN THE CREATIVE PROCESS

The authorities in Sections II.A and II.B instruct that copyright law will attribute authorship to creators who outsource the execution of their conception of the work to compliant human beings or to machines whose processes the creators control. But that discussion leaves open the question of how to analyze the results when creators allow their control over the work's execution to dissipate. For example, what of creators who intentionally incorporate random forces into the process of executing the work?⁷¹ These creators strain the boundaries of both elements of authorship: they challenge us to spurn line-drawing between authors who maintain control over outside forces and those who cede "too much" control to natural or other unmastered causes. They also push us to recognize that the "conception" prong does not require that the author have formed an exact pre-fixation conception of what the work will look like.⁷² For example, Jackson Pollock could not have anticipated the precise trajectory and landing points of the paints, even though his splatter painting process was, despite appearances, highly controlled;⁷³ yet copyright law would not doubt his authorship of his occasionally aleatory

70. *Geshwind*, 734 F. Supp. at 650–51 (noting that Geshwind's failed attempts to control Leich's creative process "[did] not make him the creator" and that "[t]he artist, Leich, is the creator").

71. See Alan R. Durham, *The Random Muse: Authorship and Indeterminacy*, 44 WM. & MARY L. REV. 569, 596–607 (2002) (discussing the use of randomness and chance in the art of Jean Arp, Marcel Duchamp, Jackson Pollock, Max Ernst, and John Cage).

72. See *infra* Section II.D (discussing imprecise or incomplete "conceptions" of a work).

73. Interview by William Wright with Jackson Pollock, in *The Springs*, Long Island, NY (1950), reprinted in JACKSON POLLOCK: INTERVIEWS, ARTICLES, AND REVIEWS 20–23 (Pepe Karmel ed., 1999). The painter Max Ernst employed an even more random process: he "[swung] a paint can with a pin-hole in it at the end of a string" to create the "elliptical linear patterns" in his work *Young Man Intrigued by the Flight of a Non-Euclidean Fly*. William Rubin, *Jackson Pollock and the Modern Tradition*, in JACKSON POLLOCK: INTERVIEWS, ARTICLES, AND REVIEW 167–68 (Pepe Karmel ed., 1999).

output.⁷⁴ But if copyright theory tolerates some degree of randomness in a work's execution, is there a point at which the putative author has surrendered so much control over the execution that the independence of the work's embodiment calls into question whether her initial conception of the work was anything more than a general idea?

Consider two versions of the “Monkey Selfie” controversy. Version One, widely reported on the Internet,⁷⁵ recounts that nature photographer David Slater was photographing macaques in a wildlife reserve in Indonesia, when “Naruto,” a particularly curious monkey, snatched Slater’s camera away, and began snapping pictures, including the remarkably accomplished self-portrait that quickly garnered viral celebrity. Version Two, as told by Slater,⁷⁶ counters that Slater had been studying the macaques in the reserve; realizing that the monkeys had been observing his activities, but would not cooperate in a portrait-sitting, Slater positioned the camera to frame the shot, including setting lighting and perspective, and waited for a curious monkey to come along, stare at the camera, and push the button, which Naruto obligingly did. The consequences of Version One for copyright are clear: merely supplying the camera does not make one an author.⁷⁷ Because Naruto not only pushed

74. See Morgan M. Stoddard, *Mother Nature as Muse: Copyright Protection for Works of Art and Photographs Inspired By, Based On, Or Depicting Nature*, 86 N.C. L. REV. 572, 578 (2008) (assuming that Jackson Pollock’s famous *Autumn Rhythm* is a protectable work).

75. Sarah Jeong, *The Monkey Selfie Lawsuit Lives*, VERGE (Apr. 13, 2018), <https://www.theverge.com/2018/4/13/17235486/monkey-selfie-lawsuit-ninth-circuit-motion-to-dismiss-denied> [perma.cc/EY6C-67SK] (“Back in 2011, nature photographer David Slater left some camera equipment out in the Indonesian rainforest. By Slater’s account, an enterprising Sulawesi crested macaque . . . picked up a camera and took a selfie.”); see also Plaintiff Naruto’s Combined Opposition to Defendants’ Motions to Dismiss at 3, *Naruto v. Slater*, No. 15-CV-04324-WHO, 2016 WL 362231 (N.D. Cal. Jan. 28, 2016) (“In or around 2011, Naruto found an unattended camera brought into Naruto’s habitat by [David] Slater. Using that camera, Naruto took a series of photographs of himself . . . through a series of purposeful and voluntary actions that were entirely unaided by Slater.”).

76. Julia Carrie Wong, *Monkey Selfie Photographer Says He’s Broke: I’m Thinking Of Dog Walking*, GUARDIAN, July 12, 2017, <https://www.theguardian.com/environment/2017/jul/12/monkey-selfie-macaque-copyright-court-david-slater> [perma.cc/P863-KAZZ] (noting that Slater “has long maintained that the selfies were the result of his ingenuity in coaxing the monkeys into pressing the shutter while looking into the lens, after he struggled to get them to keep their eyes open for a wide-angle close-up”); *id.* (quoting David Slater) (“It wasn’t serendipitous monkey behavior . . . It required a lot of knowledge on my behalf, a lot of perseverance, sweat and anguish, and all that stuff.”).

77. See *Nottage v. Jackson* [1883] 11 QBD 627, 636 (Eng.) (Bowen L.J.) (“I think it is evidently not . . . the man who contributes the machinery . . . [who] can be considered the artist.”); see also *Naruto v. Slater*, No. 15-CV-04324-WHO, 2016 WL 362231 (N.D. Cal. Jan. 28, 2016).

the button, but also selected the subject (himself), positioned himself and the camera, and framed the image, only he originated the conception (to the extent he had one) and the execution of the image. But copyright's human authorship precept precludes assigning authorship to proximate primates or other species of creators.⁷⁸

As for Version Two, Slater's role perhaps resembles Sarony's. Recall that Sarony neither pushed the shutter nor selected the precise moment to seize the image. But he did designate the photograph's subject, pose him, arrange other accoutrements and light, and frame the image. While Slater knew neither which of the monkeys he had been observing would wander over to the camera, nor how the monkey would pose before pushing the button, his initial setup of the equipment and partial definition of the resulting image constituted the formulation of a creative plan for the photographs' creation.⁷⁹ When Naruto pushed the button on the camera, the curious macaque perfected Slater's creative plan and "executed" the work on behalf of Slater, just like Sarony's camera operator.⁸⁰ In other words, although he left some elements to chance, many specifics of the grand design and most of its implementation remained Slater's.

Naruto Version Two nudges an intuitive borderline between copyrightable reining in of randomness and unprotected surrender of control. The Seventh Circuit, in its much-debated *Kelley v. Chicago Park District* decision,⁸¹ confronted that line in a controversy involving "Wildflower Works," a work whose creator, Chapman Kelley, described as "natural canvases of Kelley-designed color patterns"⁸² formed by wildflowers sprouting in oval-shaped flower beds. The court characterized the work as "a living garden" and ruled it "lacks the

78. See sources cited *supra* note 26 (discussing the human authorship requirement).

79. See *infra* Section II.D (discussing the conception requirement and its definition as a "creative plan" for the work's creation).

80. See *supra* Section II.A (discussing *Burrow-Giles* and noting the role of Sarony's camera operator).

81. *Kelley v. Chicago Park District*, 635 F.3d 290 (7th Cir. 2011). For commentary, see, e.g., Jani McCutcheon, *Shape Shifters: Searching for the Copyright Work in Kinetic Living Art*, 64 J. COPYRIGHT SOC'Y U.S.A. 309 (2017) [hereinafter McCutcheon, *Shape Shifters*]; Jani McCutcheon, *Natural Causes: When Author Meets Nature in Copyright Law and Art. Some Observations Inspired by Kelley v. Chicago Park District*, 86 U. CINN. L. REV. 707 (2018) [hereinafter McCutcheon, *Natural Causes*]; Joseph P. Liu, *What Belongs in Copyright*, 39 COLUM. J.L. & ARTS 325, 329–32 (2016) (discussing *Kelley*, 635 F.3d 290).

82. *Kelley*, 635 F.3d at 293.

kind of authorship and stable fixation normally required to support copyright.”⁸³

[W]orks owing their form to the forces of nature cannot be copyrighted. . . . Most of what we see and experience in a garden—the colors, shapes, textures, and scents of the plants—originates in nature, not in the mind of the gardener. At any given moment in time, a garden owes most of its form and appearance to natural forces, though the gardener who plants and tends it obviously assists. All this is true of Wildflower Works, even though it was designed and planted by an artist.⁸⁴

The court distinguished Jeff Koons’ “Puppy,” a topiary composed of individually-selected flowers planted in meshwork to fill out the canine form. “Puppy” may be a sculpture; Wildflower Works “is quintessentially a garden.”⁸⁵ Many have criticized the court’s perception that natural forces dictated the appearance of Wildflower Works; they contend that the court failed to appreciate Kelley’s intervention in studying seed and wind patterns and preparing the soil to accommodate seasonal seed arrivals that would produce particular color patterns.⁸⁶ The court and its critics do not in fact differ on the terms of debate: how much control did Kelley exercise over the creative process?⁸⁷ For the court, the garden was “conceptual art,” i.e., a mere idea (flowers forming color patterns), whose actualization did not owe its origin to Kelley, but rather to Mother Nature. For its critics, Kelley had thought through the particular color patterns that the seasonal wildflowers would embody (detailed conception), and he sufficiently—if not minutely down to the last flower like Koons—controlled the patterns’ execution by anticipating and to some extent manipulating natural forces. Were actual control irrelevant, as some advocates of conceptual art might urge,⁸⁸ the Seventh Circuit’s critics

83. *Id.* at 303–04 (“[T]he law must have some limits; not all conceptual art may be copyrighted. In the ordinary copyright case, authorship and fixation are not contested . . . [b]ut this is not an ordinary case. A living garden like Wildflower Works is neither ‘authored’ nor ‘fixed’ in the senses required for copyright.”).

84. *Id.* at 304 (citations omitted).

85. *Id.* at 304–06.

86. *See, e.g.,* McCutcheon, *Natural Causes*, *supra* note 81, at 709 (noting that the Seventh Circuit “failed to give sufficient weight to [Chapman Kelley’s] selection and arrangement, . . . wrongly allocating to nature the primary responsibility for the material form of the work”).

87. *See* Shyamkrishna Balganes, *Causing Copyright*, 117 COLUM. L. REV. 1, 31 (2017) (characterizing the flaw in Kelley’s claim as a failure of “control over the creative process”).

88. *See* Durham, *supra* note 71, at 597–98 (noting how Jean Arp “tipped [the] balance between accident and deliberation more than usual in the direction of accident” and sought to

would not be seeking to construct the facts to enhance Kelley's determinative role in the formation of the color patterns; it would suffice that he conceived the garden's grand design, of which the delegation of its execution to natural forces may have been an essential component.

Finally, an example of "conceptual art" that most likely joins *Naruto Version One* on the authorless side of the line, rather than straddling it, as did *Kelley* or *Naruto Version Two*. The artist Agnieszka Kurant produces brightly colored sculptures by feeding primary-colored crystals to termites, who then build mounds in the colors of the crystals they ingest and then excrete.⁸⁹ Apart from providing the colors, Kurant exercises no control over the vaguely phallic forms the termites construct. Thus, Kurant formulates a creative plan whose execution she leaves almost entirely to faunal forces. At the front end, conception, her study of termite activity might enable her to anticipate unspecified overall shapes; at the back end, execution, she contributed solely the color component of the building materials (akin to supplying the film for the photographer's camera). Her role implicates scarcely more input than the *Little Prince's* command to "Draw me a sheep!" But, from a copyright law perspective, where the aviator could claim the mantle of authorship, the termites' output yields an authorless production. Kelley's garden and Kurant's termite mounds serve as reminders that the copyright law's notions of authorship may at times diverge from the art world's.

abandon "conscious volition" in his art as an "exercise in self negation" (citing Jane Hancock, *Arp's Chance Collages*, in *DADA/DIMENSIONS* 47 (Stephen C. Foster ed., 1985)).

89. Agnieszka Kurant, *Phantom Capital, Hybrid Authorship, and Collective Intelligence*, 39 *COLUM. J.L. & ARTS* 371, 371 (2016) (describing the artist's piece entitled "*A.A.I.*, which stands for Artificial Artificial Intelligence," whose creation the artist "outsourced to another species—to the colonies of living termites" and noting that "there [was] no way of telling in advance what the final shape [would be]" because the mounds' structure "emerg[es] through millions of micro-contributions by [the] insects").

Figure 1: Agnieszka Kurant’s “A.A.I” or “Artificial Artificial Intelligence”⁹⁰



D. THE LIMITS OF THE AUTHOR’S “CONCEPTION”

One might imagine that an author’s “conception”—her *mental* work, as distinguished from her execution or *physical* work⁹¹—consists of the pre-execution formulation of an overall perception of the finished product. This notion of conception reflects the traditional mode of authorship: the novelist or artist who first envisions a work and then employs her skill to transfer it from the mind’s eye to the canvas or the page. We have shown that the principles underlying copyright’s execution requirement accommodate modes of authorship outside this model: the author who removes herself from the physical process of creation, relying on mechanical tools, amanuenses, or natural forces, does not necessarily forego authorship status.⁹² In this Section, we argue that copyright’s conception requirement also accommodates modes of creation outside the traditional model, and propose a definition of the conception requirement that fits all analog authorship contexts.

1. *Curing Deficiencies in Conception: The “Adoption” Theory of Authorship*

Section II.C suggests that an “author” need not maintain absolute control over the execution of her work and may instead rely on external forces, like randomness and nature, to complete her work, so long as she bends those forces to her will. By the same token, those processes may develop the work in ways that the author did not conceive in detail before their intervention. If

90. Nicole Walsh, *Meet the Woman Making Art with Termites; Polish artist Agnieszka Kurant outsources her labor to an unsuspecting insect army*, VICE (Aug. 7, 2015), https://creators.vice.com/en_us/article/8qvmwz/meet-the-woman-making-art-with-termites [perma.cc/L647-LHXK].

91. *See supra* Sections II.A–C.

92. *See id.*

copyright law nonetheless accepts the creator's authorship, it follows that copyright's "conception" requirement does not oblige the author to formulate a complete and accurate mental image of the work *before* she applies her hand (or directs another's hand) to executing it.

Judge Jerome Frank in *Alfred Bell & Co. v. Catalda Fine Arts*⁹³ offered a proposition that expands on this basic principle. The case concerned originality in mezzotint engravings of old master paintings. The defendant had claimed that the prints, as copies of public domain works, could not enjoy copyright protection for lack of originality. The court rejoined that the differences the engravers introduced in transforming the oil paint originals into printed renditions yielded sufficient "distinguishable variations" to support a copyright. The court then speculated:

A copyist's bad eyesight or defective musculature, or a shock caused by a clap of thunder, may yield sufficiently distinguishable variations. Having hit upon such a variation unintentionally, the "author" may adopt it as his and copyright it.

Plutarch tells this story: A painter, enraged because he could not depict the foam that filled a horse's mouth from champing at the bit, threw a sponge at his painting; the sponge splashed against the wall and achieved the desired result.⁹⁴

If copyright extends only to works deliberately conceived and purposefully executed, then the creator's after-the-fact recognition of the value in his "mistake" supplies the missing element required to vest the outcome with the stamp of authorship.⁹⁵ This authorship-by-adoption approach acknowledges that the author may deliberately revise her initial conception or creative plan to include her slip of the pen.⁹⁶ Adoption theory recognizes that authorial acts need not occur in a particular order: first with a detailed conception, and then with the conferral of concrete form on the conception. Rather, by "discovering" the aesthetic value of an expressive element that the author has unintentionally brought into being, and deciding to "adopt" it as her own expressive creation, an author is contemporaneously revising her conception of the work. To return to Judge Frank's examples, the changes wrought by the

93. *Alfred Bell & Co. v. Catalda Fine Arts*, 191 F.2d 99, 105 (2d Cir. 1951).

94. *Id.* at 105 n.23.

95. *Id.*

96. *Id.* Incorporating an accidental element—the product of happenstance, luck, or pure chance—into one's creative plan is no more offensive to the principle of conception than an artist's purposeful deployment of randomness. See *supra* Section II.C (discussing the use of randomness in art).

clap of thunder may yield an image the author had not expected to draw; their adoption modifies her conception of the work. In the Plutarch anecdote, the painter imagined foam at the mouth of the horse, but could not envision it with sufficient precision to render it physically. The flung sponge enabled the artist to see (as well as unintentionally to execute) what he had sought.⁹⁷

Ultimately, authorship-by-adoption is an instance of a broader proposition: “conception” in copyright law does not mean that the work must, Athena-like, spring fully-formed from the head of the author. The author remains an author even if, during her execution of a work, she deviates from her initial expectations, whether to accommodate an unforeseen and unintentional development, or simply because her ideas have evolved in the course of creating the work.⁹⁸ An author might find that her characters have run away with the story, compelling different plot developments;⁹⁹ she might fling a sponge at her canvas in frustration and prefer the resulting splatter to anything she could have achieved with the brush; or she might accidentally knock over a paint can, spilling paint on her pointillist depiction of a seaside landscape, only to discover in Abstract Expressionism her true calling. In effect, the author’s execution *perfects* her mental conception.

Authorship-by-adoption, however, makes sense only if the “adopter” also performed or directed the work’s execution. If authorship-by-adoption is the post-fixation revision of an author’s “conception” to include an accidental variation, then the theory does not help the creator who cannot claim authorship due to her lack of execution. Consider *Naruto Version One*.¹⁰⁰ If the monkey grabs the camera and takes the selfies, the photographs result from a supervening cause.¹⁰¹ If Slater decides that one of the primate-generated

97. Judge Frank’s examples also illustrate adoption of changes occurring when the author lost some control over her execution of the work. In these examples, the author in fact carried out the acts of execution, but the acts were not contemporaneously willed. By adopting the results, however, the author makes the supervening cause her own, thus overcoming her loss of control at the time of execution.

98. See Nathan Israeli, *Creative Processes in Painting*, 67 J. GEN. PSYCHOL. 251, 251–56 (1962) (detailing a “self-observation study of oil painting” during which the author painted “without previous planning or preparation, and without any sketch, design or imagery,” describing how the author “checked” his painting “operations” as he “pause[d] to look at the painting from close at hand or from a distance” during the process of creation, and that this constant “[c]heck and evaluation of the operations and outcomes [were] followed quite often by plans, suggestions, and decisions which control the subsequent operations on the painting”).

99. Cf. LUIGI PIRANDELLO, *SIX CHARACTERS IN SEARCH OF AN AUTHOR* (1921) (absurdist play in which the characters’ search for the play’s author drives the play’s plot).

100. See *supra* notes 75–77 and accompanying text (describing *Naruto Version One*).

101. Balganes, *supra* note 87, at 3–4 (discussing the *Naruto* case and arguing that “Slater’s failure to press the shutter button himself . . . broke[] his causal connection to the work”).

images corresponds to the photograph he had hoped to take, and therefore adopts it as his own, does that suffice to make him the author? Instinctively, we are likely to resist that conclusion. There is a salient difference between Slater (in this version) and Plutarch's painter: the painter did not intend or expect to achieve his desired pictorial result by flinging the sponge, but he both intended to and did throw the sponge against the wall. Slater did not himself take the picture, nor did he intend to delegate the picture-taking to the monkey.

Applying adoption theory to post-fixation selection among outputs the putative author did not herself directly or indirectly bring forth leads to implausible outcomes. Suppose the person who supplies and sets up a camera and instructs it to take pictures at predetermined intervals is not the same person as the person who selects which of the outputs to claim. For example, a security camera indiscriminately and continuously captures all that comes within the camera's sights; a third party selects an image from the thousands the camera fixed. If security camera images so lack originality as to fit the *Sarony* court's evocation of the "ordinary production of a photograph,"¹⁰² they might not qualify as "writings" of "authors." Post-execution selection in this scenario would then supply the only authorial act. But without participation in the creation (initial conception and fixation) of the image, merely choosing a previously fixed image should not suffice to confer authorship status on the person making the selection. Otherwise, for example, a police officer who

102. *Burrow-Giles Lithographic Co. v. Sarony*, 111 U.S. 53, 55–59 (1884). Courts have not yet addressed whether security camera images fit within the category of "ordinary production[s] of a photograph." The issue came up in a case which did not reach a final decision on the merits. *See* Defendant's Motion for Summary Judgment at 4–6, *Southwest Casino & Hotel Corp. v. Flyingman*, No. CIV-07-0949 (W.D. Okla. Aug. 28, 2008) (arguing that the plaintiff's video, taken from plaintiff's surveillance camera footage, lacked sufficient creativity for copyright). Courts and commentators have expressed some doubt regarding the continued significance of the *Burrow-Giles* "ordinary production" language. *See* *Mannion v. Coors Brewing Co.*, 377 F. Supp. 2d 444, 450 (S.D.N.Y. 2005) (noting that "[a]lmost any photograph 'may claim the necessary originality to support a copyright'"). The U.S. Copyright Office's most recent compendium does not address the issue of what constitutes the "ordinary production of a photograph." *See* COMPENDIUM, *supra* note 25, at § 909.1 ("The creativity in a photograph may include the photographer's artistic choices in creating the image, such as the selection of the subject matter, the lighting, any positioning of subjects, the selection of camera lens, the placement of the camera, the angle of the image, and the timing of the image."). Assuming that security camera footage displays at least some of the characteristics listed in the compendium as elements of creativity in photography, it may well be registrable.

combs through the security camera's images searching for a good likeness of a suspect, would, on finding such an image, become its author.¹⁰³

Were post-execution adoption to substitute for any authorial participation, even indirect or inadvertent, in giving physical form to a work, then, in addition to designating the “wrong” author, copyright law would effectively vest adopters with rights in ideas. Ponder “Fountain,” Marcel Duchamp’s 1917 pedestal-mounted urinal. Duchamp did not create a replica of a urinal; he adopted an actual plumbing fixture, and “gave it a new context” by setting it in a gallery.¹⁰⁴ Duchamp may have created the context, that is, he may have come up with a provocative and art history-altering idea, but he did not create the readymade urinal.¹⁰⁵

2. *Conception via Process*

But what if an author creates something unexpected and is not present to “adopt” the unplanned variation? If the adoption theory contemplates an author deliberately altering her conception or “creative plan” in order to subsume an unplanned variation, then an author who never sees the unplanned

103. If the officer selected several photos from the full output, the selection might make her the author of a compilation of the photos, but copyright in the compilation does not extend to the underlying elements. See 17 U.S.C. § 103(b) (2018).

104. An unsigned editorial in the second issue of *The Blind Man*, published on May 17, 1917, explains in support of *Fountain*: “He took an ordinary article of life, placed it so that its useful significance disappeared under the new title and point of view—created a new thought for that object.” Louise Norton, *The Richard Mutt Case*, BLIND MAN, May 1917, at 5, <http://sdr.lib.uiowa.edu/dada/blindman/2/05.htm> [perma.cc/6RD4-BRFS].

105. But see Laura A. Heymann, *A Tale of (At Least) Two Authors: Focusing Copyright Law on Process Over Product*, 34 J. CORP. L. 1009, 1015 (2009) (“Marcel Duchamp is the ‘author’ of *Fountain* (1917), a ‘readymade’ sculpture consisting of a urinal, because he has declared his effort to be art.”). Also consider the hypothetical presented by Alan R. Durham in *The Random Muse: Authorship and Indeterminacy*: an artist discovers a pattern on the “floor of a hardware store, where generations of customers had dripped paint . . . purchase[s] that section of the floor,” and “[hangs] it in her gallery.” Durham, *supra* note 71, at 624–25. Professor Durham notes that this case “resembles that [of the artist in *Bell v. Catalda*, 191 F.2d 99], with the difference that [Durham’s hypothetical artist] had no physical role in the creation of the work she ‘adopted.’” *Id.* The artist’s selection nonetheless “reflects her tastes and proclaims her individual vision.” *Id.* Durham concludes that the artist “might advance a claim [of copyright]” based on having “improved the commons” by “singling out this section of floor as one with expressive potential,” and that “awarding [the artist] exclusive rights would promote the progress of the arts.” *Id.* But extending copyright to an output because protection will achieve some of the copyright system’s goals puts the cart before the horse: first we must ascertain whether the object at issue is a work of authorship, i.e., whether its putative author actually executed it. The object does not become a work of authorship merely because vesting its claimant with exclusive rights leads to results consonant with at least some theories of copyright law.

variation cannot utilize the theory retroactively to reconceptualize the work. Suppose Naruto Version Three: Slater positions his camera in the jungle with all the chosen settings, pushes a button that releases the shutter at timed intervals, leaves the scene, but never returns. Later, a competing photographer discovers Slater's abandoned camera and the images captured in its memory, and selects one to publish in National Geographic. The competing photographer has no greater claim to authorship of the selected photograph than does the police officer who selects among images captured by a security camera, posited earlier. Neither the rival photographer nor the police officer in any way participated in the execution of the photos.

But what about Slater's claim to authorship? Suppose that in Version Three Slater's camera captured some other denizen of the wildlife preserve unexpectedly attacking and eating Naruto. The resulting image would be very different from the image Slater thought he would capture. Can Slater claim authorship over the photograph even though he did not, at the time of execution, know precisely what image he would end up producing? If he leaves the scene (and his camera), never to return, Slater has no subsequent opportunity to bolster his claim to authorship by "adopting" the final image; does it follow that his failure to ratify the actual result deprives him of authorship over the image?

We intuitively sense that Slater (like all photographers) is the author of the images he executes, even if his anticipation of what he might capture is vague or proves inaccurate. Case law and professional practice¹⁰⁶ have confirmed our intuition:¹⁰⁷ many photographers and cinematographers capture events which they did not anticipate, and courts seem content to recognize them as authors despite the disjunction between expectations and outcomes. When Abraham

106. This version of the Naruto hypothetical mirrors the process many nature photographers and documentarians use to produce their works. See, e.g., *Filming the 'Impossible': Sets, Filming Burrows, and Tanks*, BBC EARTH (Apr. 29, 2016), <http://www.bbc.com/earth/story/20160310-filming-the-impossible-sets-filming-burrows-and-tanks> [perma.cc/KSS8-B5ZW] (noting the use of remote cameras to produce the footage for BBC's Frozen Planet nature documentary).

107. For example, the U.S. Copyright Office notes that the "author and initial copyright owner of a photograph is generally the person who 'shoots' or 'takes' the photo" and that the copyright in a photograph "protects the photographer's artistic choices, such as . . . the selection of camera lens, the placement of the camera, the angle of the image." UNITED STATES COPYRIGHT OFFICE, COPYRIGHT REGISTRATION OF PHOTOGRAPHS, CIRCULAR 42 (2018), <https://www.copyright.gov/circs/circ42.pdf> [perma.cc/647K-8ST3]. The Copyright Office thus does not inquire whether the putative author of a photograph possessed a sufficiently accurate pre-execution conception of what the photograph might contain, or whether the author sufficiently "adopted" the unintended elements post-execution.

Zapruder, “by sheer happenstance” captured a film of President Kennedy’s assassination in 1963 which later became the subject of litigation in the Southern District of New York, the court did not question Zapruder’s claim of authorship over the footage, even though Zapruder’s intention was to “tak[e] home movies” of the presidential motorcade, not to create a “historic document” depicting Kennedy’s death.¹⁰⁸

If we accept that Slater (Naruto Version Three) is the author of his photographs, but we also posit that all authors must “conceive” of their works, then Slater’s “conception” of his work must consist of something other than precise anticipation of the contents of his photographs. Unlike Sarony,¹⁰⁹ Slater and other nature photographers “conceive” of their works not by composing the photograph to reflect a fully developed view of the resulting work, but by formulating a set of deliberate executional steps (setting up a particular type of camera in a particular location, at a particular time, with a particular type of lens, etc.), which will lead to the generation of a work, the precise composition and contents of which they cannot foresee. Like many contemporary artists, the nature photographer’s “conception” consists entirely of her definition of her *creative process*.¹¹⁰

Like the archetypal author, nature photographers and other process-based authors generate a conception that guides their execution of the work. But

108. *Time Inc. v. Bernard Geis Assocs.*, 293 F. Supp. 130, 131 (S.D.N.Y. 1968).

109. By “posing the said Oscar Wilde in front of the camera, selecting and arranging the costume, draperies, and other various accessories in said photograph, arranging the subject so as to present graceful outlines, arranging and disposing the light and shade, [and] suggesting and evoking the desired expression,” Sarony composed his work to match his mental image of the photograph he sought to create. *Burrow-Giles Lithographic Co. v. Sarony*, 111 U.S. 53, 60 (1884).

110. See, e.g., KIM GRANT, *ALL ABOUT PROCESS: THE THEORY AND DISCOURSE OF MODERN ARTISTIC LABOR* (2017) (quoting Chuck Close) (“I really did believe that process would set you free. . . . A signature style is about how it happened, not what is made. I think of myself as an orchestrator of experience.”); *id.* (noting the “elevation of artistic process over product,” that “many artists consider themselves to be primarily engaged with process,” and that “[a]ccompanying the recent prominence of artistic process is a corresponding decline of the artist’s product as an object of independent aesthetic interest”). Steve Reich, a minimalist composer, provided an apt example of process-based art in his piece *Pendulum Music*. Reich hung “some microphones from the ceiling on very long cords and put them over loud speakers and set them in motion swinging as pendulums.” Robert W. Clarida, *Copyrightability of Conceptual Art: An Idea Whose Time Hasn’t Come*, 39 COLUM. J.L. & ARTS 365, 369 (2016). As the “pendulums” “cross the loud speakers they make a sound,” and as several pendulums move “at once,” going “in and out of phase with each other,” they collectively produce the musical work. *Id.* Reich described his piece as an example of “music as a gradual process.” See Steve Reich, *Music as a Gradual Process and Pendulum Music*, in *MUSIC OF THE AVANT-GARDE 1966–1973* 317 (Larry Austin, Douglas Kahn & Nilendra Gurusinghe, eds., 2011).

unlike the traditional author, these authors' conceptions do not involve a pre-existing "vision[] of what the [work] should look [or sound] like."¹¹¹ Their pre-fixation conceptions instead concern what the work *could* become and *how* it will come into physical being. The elements in the resulting work flow directly¹¹² from the choices the author makes when developing her creative plan.¹¹³ Once the photographer completes that creative plan by generating a photograph, her execution of the work perfects her "conception" and vests her with authorship, even if she does not ratify the result. When those photographers are "astonish[ed]" by the unanticipated contents of the resulting footage (which might reveal patterns of faunal behavior previously unknown to the authors or the scientific community as a whole),¹¹⁴ the dissonance between the images the photographers may have envisioned before execution and the final images does not disqualify them from claiming authorship because their authorship already vested at the moment the photograph's execution occurred. Accordingly, an author who devises such a creative plan and subsequently executes it is presumptively the author of the final work. If a putative author's sole execution of a work is uncontested, and if there is no reason to believe that anyone other than the putative author

111. *Lindsay v. The Wrecked and Abandoned Vessel R.M.S. Titanic*, No. 97 Civ. 9248 (HB), 1999 WL 816163, at *5 (S.D.N.Y. Oct. 13, 1999).

112. One might object that the nature photographer's actions and "creative plan" does not *entirely* determine the expressive content of the resulting images because forces of nature, operating in front of the camera's lens, are the origin of the resulting image's content. But the influence of an external force like nature or randomness does not destroy a creator's right to claim authorship. *See supra* Section II.C. Even though the contents of the nature photographer's image might depend on which animals happen to wander into her camera's viewfinder, the photographer's creative plan—to capture an image of the goings-on in front of her camera, on a particular type of film and according to a particular set of camera parameters—is complete no matter the ultimate contents of the image. Unlike Chapman Kelley or Agnieszka Kurant, the nature photographer is solely responsible for the execution of her work and has not ceded control over that physical process to nature. Only if an unforeseen event supersedes the photographer's execution, for example, if a third party were to press the shutter before the auto-timed setting, would we call into question the photographer's authorship claim.

113. *See Durham, supra* note 71, at 637 (noting that authorship requires a "minimal exercise of 'creative control'" which Durham defines as "choices made by the author that are reflected in the form of the work," choices which "might be made before the fact, as when John Cage established the rules of one of his indeterminate systems, based on star atlases or the *I Ching*, only to let chance take over in determining the ultimate form of the composition").

114. Emma Bryce, *Behind the Scenes of BBC America's Planet Earth II*, AUDUBON (Feb. 17, 2017), <https://www.audubon.org/news/behind-scenes-bbc-americas-planet-earth-ii> [perma.cc/2EQ8-F6RQ] (describing how the team of cinematographers behind BBC America's recent nature documentary worked "hand in hand with biologists" for "months" in order to capture "footage of undiscovered interactions between wildlife," including "astonishing" footage of a Bird-of-Paradise in a rarely seen mating dance).

generated the creative plan that guided that execution, then there is no need to investigate whether she adequately “conceived of” the work.

Situations of contested authorship arise when there is some reason to doubt whether the person claiming authorship both developed the creative plan behind the work, and executed (or controlled the execution of) that plan. As discussed in Section II.C, if an artist fully develops a creative plan or conception for a work (as Chapman Kelley surely did for Wildflower Works), but does not control the execution of that plan (instead delegating the execution to a force beyond the author’s control), the artist may not be an “author” in the copyright law sense. In addition, when multiple putative authors contribute to a work’s execution, copyright law must provide a mechanism for determining who among the claimants is responsible for generating the creative plan behind the work, and for controlling the execution of that plan. To that scenario we now turn.

E. ALLOCATING AUTHORSHIP BETWEEN UPSTREAM AND DOWNSTREAM AUTHORS

To this point, we have addressed scenarios featuring only one human author. These have presented binary outcomes: sufficiently detailed conception and controlled execution, or not. We now analyze situations in which different humans contribute to the work’s execution, where both have a colorable claim to have generated the work’s conception. We posit four scenarios:

- (i) The upstream creator¹¹⁵ remains the sole author because she has controlled the downstream contributor’s process of execution and reduced the latter either to a “mere amanuensis,” or to selecting among outcomes the upstream contributor has anticipated and built into the work.
- (ii) The downstream creator is the sole author of the resulting work because the upstream creator has provided only an unprotectable idea, which the downstream creator has elaborated into a detailed conception which she has embodied in physical form (e.g., “draw me a sheep”).

115. By “upstream creator” we mean a participant in the process who contributes to the work’s creation, but does not cause the final manifestation of the work. For example, Sarony set the scene and posed Oscar Wilde, but he did not operate the camera. See *Burrow-Giles*, 191 F.2d at 105. By “downstream creator” we mean the person responsible for the last steps required to create the work. Sarony’s cameraman filled that role by choosing when to press the shutter to fix the image.

(iii) The upstream and downstream creators have collaborated with the intent to merge their individual contributions (conception and execution) into a unitary whole, and are thus co-authors of a joint work.¹¹⁶

(iv) The upstream and downstream authors both contribute to the creation of the work, but they fail to qualify as co-authors.¹¹⁷ Whether either or both would individually be authors of their contributions depends on whether either or both contributions would independently qualify as an original work of authorship.

Mere amanuenses supply the clearest example in the first category; the principal author has outsourced the execution of her fully-formulated conception, leaving little room for the executor to impose her own conception on the work upon its execution. For example, Alexander Calder did not personally weld his monumental stabiles; metal workers at Segre Iron Works performed the task.¹¹⁸ Calder would supply “sketches of his stabiles — abstract constructions evocative of movement,”¹¹⁹ leaving it to the welders to “figure [] out” how to execute the work in iron. Nonetheless, the artistic vision remained Calder’s alone: “If he says it isn’t right, we do it over and over again until he’s pleased with it.”¹²⁰

But in other instances, the upstream contributor may not be standing over the shoulder of the downstream actor. Leaving the scene, she may present him with a range of possibilities, to choose among the branches of a decision tree. Thus, even though the upstream actor does not conclusively determine the form of the resulting work, by defining its key expressive elements, she remains the “mastermind” of the work, and effectively executes it by constraining the options through which the downstream actor will bring the final form of the work into being. In other words, while the downstream actor executes the work, he does not contribute to the work’s conception—the upstream actor is solely responsible for the creative plan behind the work. The fewer the options, the less likely any attribution of authorship of the output to the downstream actor. But, by the same token, the more choices allowed the downstream actor, the greater his claim to be an author of the output. This Section considers a range of examples to test whether the upstream actor has sufficiently bounded the downstream actor’s choices to retain the crown of sole authorship.

116. See *infra* Section II.F for a discussion of the rules of co-authorship and whether the upstream and downstream contributors can claim to have together created a “joint work.”

117. *Id.*

118. See Michael Knight, *Constructing a Calder Is a Labor of Love*, N.Y. TIMES, Feb. 9, 1974, <https://www.nytimes.com/1974/02/09/archives/constructing-a-calder-is-a-labor-of-love.html> [perma.cc/D47Y-P45X].

119. *Id.*

120. *Id.* (quoting Frank Pisani, the foreman at Segre Iron Works).

Suppose that an author produces a “choose your own adventure” ebook. Every few pages, the author instructs the reader to choose between several options which lead the reader to different resulting storylines (e.g., “To take the blue pill, click here; to take the red pill, click here,” etc.). When the reader has made the last of multiple choices, the ebook device preserves a full copy of the storyline reflecting the user’s choices, thus fixing the reader-generated sequence in a tangible medium. We might conclude that the reader is not the author of the sequence because he has contributed nothing that the initial author has not foreseen; the author has preset the content of each option, and the combinations of options, though numerous, remain a very finite universe.

Now consider a kaleidoscope. The kaleidoscope’s designer selects the colors and shapes of the shards of glass or paper that, when the viewer turns the outer cylinder, will form patterns, multiplied by the reflecting panels in the inner cylinder. Suppose also that the designer attaches the kaleidoscope to a camera, which fixes an image of the kaleidoscope’s output every time the user turns the cylinder. The number of possible patterns will depend on the amount and shapes of the materials inside the cylinder, but sooner or later, patterns will reappear. Even if the kaleidoscope’s designer did not anticipate every potential image output, the possible combinations remain finite. Moreover, by choosing the color scheme and the shapes of the components, as well as the size of the fractal patterns, the designer has selected the key aesthetic effects of the kaleidoscope. Finally, although the user turns the outer cylinder, thus causing the patterns to appear, the user will have made no intellectual contribution to the output. Here we can attribute sole authorship of the fixed images of the various patterns to the designer, not only because the user’s contribution bears no stamp of authorship, but because there is no combination of pattern-producing elements that was not inherent in their initial selection and mode of presentation. In other words, while the designer of the kaleidoscope may not have anticipated each potential output, the designer formulated a *complete* creative plan which would result in a fully-formed work (or many fully-formed works, with each turn of the tube).

The kaleidoscope scenario resembles the facts of a series of cases from the 1980s concerning early videogames.¹²¹ The defendants copied the games’ audiovisual output and claimed the works were not sufficiently fixed to qualify for copyright because the exact sequence of moving images depended on how users played the game. Thus, the defendants argued, the user shaped the

121. See *Stern Elecs. Inc. v. Kaufman*, 669 F.2d 852, 855 (2d Cir. 1982); *Williams Elecs., Inc. v. Artic Int’l, Inc.*, 685 F.2d 870, 874 (3d Cir. 1982).

output¹²² of the work, and the upstream game programmer could not predict the precise form and sequence of the user-manipulated audiovisual experience. Courts rejected this contention, holding that each possible gameplay sequence was incipient in the game's design. For example, in *Midway Manufacturing Co. v. Artic International, Inc.*,¹²³ the Seventh Circuit upheld the copyrightability of the audiovisual elements in classic videogames like Galaxian and Pac-Man:

Playing a video game is more like changing channels on a television than it is like writing a novel or painting a picture. The player . . . does not have control over the sequence of images that appears on the video game screen. He cannot create any sequence he wants out of the images stored on the game's circuit boards. The most he can do is choose one of the limited number of sequences the game allows him to choose. He is unlike a writer or a painter because the video game in effect writes the sentences and paints the painting for him; he merely chooses one of the sentences stored in its memory, one of the paintings stored in its collection.¹²⁴

In other words, the player could not cause the game to display any sequence that was not already built into the program, no more than the choose-your-own-adventure reader could pursue an adventure outside the built-in options, or the kaleidoscope user could generate a pattern different from the patterns the designer's selection of components and reflectors enabled.¹²⁵ In each of

122. Cf. Jani McCutcheon, *The Vanishing Author in Computer-Generated Works: A Critical Analysis of Recent Australian Case Law*, 36 MELB. U. L. REV. 915, 938 (2013) (noting that "an author can rely on another person or machine to supply the fixation effort, provided the author's mind directs and shapes the output") (citing *Donoghue v. Allied Newspapers Ltd.*, [1938] 1 Ch 106, 109 (Farwell, J)).

123. *Midway Mfg. Co. v. Artic Int'l, Inc.*, 704 F.2d 1009 (7th Cir. 1983).

124. *Id.* at 1012.

125. The "finite universe" or "inherent in the program" analyses may ultimately founder as the universe of combinations expands. Courts continue to rely on *Williams Electronics* and progeny to sustain the sole authorship of the designer of the computer game. See *Stern*, 669 F.2d at 856 (concerning a coin-operated videogame named "Scramble," and concluding that the "player's participation does not withdraw the audiovisual work from copyright eligibility"); *Midway*, 704 F.2d at 1010–11 (7th Cir. 1983) (upholding copyright in the audiovisual elements in classic videogames like Galaxian and Pac-Man). However, the force of precedent may be compensating for the thinning pertinence of those decisions' premises. See, e.g., Kyle Coogan, *Let's Play: A Walkthrough of Quarter-Century-Old Copyright Precedent as Applied to Modern Video Games*, 28 FORDHAM INT. PROP. MEDIA & ENT. L. J. 381, 401–02 (2018) (noting the videogame case precedent from the 1980s and arguing that "[i]f courts were to revisit [those cases] today, it seems possible that real-time gameplay would fall short of being a protectable audiovisual work" because some games "such as sandbox games or MMORPGs" "are much more like painting a portrait than they are like 'changing channels on a television'" because they "allow a vast array of possibilities for user interaction" and because it is "nearly impossible

these examples, the “upstream” contributor (who designs the videogame, the choose-your-own-adventure novel, and the kaleidoscope) has bound the “downstream” contributor to fulfilling a limited role within the “upstream” contributor’s completed creative plan.¹²⁶

By contrast, suppose that an author writes the beginning of a short story, which she posts on a website, inviting any and all participants to compose endings for the tale. In due course, many writers respond; the initiating author selects one of the offered endings. Who is/are the author(s) of the combined story?¹²⁷ The story’s initial plot and character development will necessarily dictate some aspects of the story’s further development and conclusion, but, unlike the previous examples, they do not foreordain all possible outcomes. The second contributor’s relative creative freedom entitles her to authorship status in her contribution. In other words, while the first writer has influenced the form and structure of the second contributor’s composition, the first writer did not fully formulate a creative plan for the completed work. The completion of the story required the second contributor’s additional creativity. But if the initiating author is not the author of the story’s ending, neither is the second contributor the author of the story’s beginning. To ascertain whether they are co-authors of the combination,¹²⁸ Section II.F turns to the question of joint works.

F. SHARING AUTHORSHIP: JOINT WORKS

1. *Categories of Joint Works and Modes of Co-Authorship*

The Copyright Act defines a joint work as “a work prepared by two or more authors with the intention that their contributions be merged into inseparable or interdependent parts of a unitary whole.”¹²⁹ The disjunctive language implies that the terms “inseparable” and “interdependent” describe distinct types of joint works.¹³⁰ All multiple-authored works are in some way

to produce an entirely similar sequence of audiovisuals from game-to-game”) (quoting *Midway*, 704 F.2d at 1012).

126. If the downstream contributor instead eschews the upstream contributor’s set parameters—for example, by disassembling the kaleidoscope or including new colors in order to change the appearance of the resulting patterns—the downstream contributor has interrupted and displaced the upstream contributor’s creative plan and, accordingly, her ability to claim authorship over the altered resulting images.

127. Hypothetical based on Jane C. Ginsburg, *Putting Cars on the “Information Superhighway”*: *Authors, Exploiters, and Copyright in Cyberspace*, 95 COLUM. L. REV. 1466, 1469–70 (1995).

128. As opposed to sole authors of their individual contributions.

129. 17 U.S.C. § 101 (2018).

130. The disjunctive language used in the legislative history describing the clause also supports this conclusion. *See* S. REP. NO. 94-473, at 103–04 (1975); *see also* H.R. REP. NO. 94-

“interdependent”—even a work created through close collaboration (e.g., Marx & Engels) requires the “interdependent” contributions of each participant. To give separate meaning¹³¹ to the words “interdependent” and “inseparable” we must confine the meaning of “interdependent” to joint works comprised of multiple distinct and independently copyrightable works.¹³² An “inseparable” joint work is therefore a work that is not capable of disaggregation into independently copyrightable parts attributable to each co-author.¹³³

The legislative history references two distinct modes of co-authorship: (i) co-authors might “collaborate[] with each other,”¹³⁴ and (ii) each author might produce her contribution independently “with the knowledge and intention

1476, at 120 (1976) (noting that “the parts [of a joint work] themselves may be either ‘inseparable’ (as the case of a novel or painting) or ‘interdependent’ (as in the case of a motion picture, opera, or the words and music of a song)”).

131. See *Colautti v. Franklin*, 439 U.S. 379, 392 (1979) (noting that it is an “elementary canon of construction that a statute should be interpreted so as not to render one part inoperative”); *United States v. Menasche*, 348 U.S. 528, 538–39 (1955) (citations omitted) (“It is our duty ‘to give effect, if possible, to every clause and word of a statute.’”).

132. See *Mapp v. UMG Recordings, Inc.*, 208 F. Supp. 3d 776, 786 (M.D. La. 2016) (noting that “parts of a unitary whole” are “interdependent” when they can have some meaning standing alone, but “achieve their primary significance because of their combined effect, as in the case of the words and music of a song”) (citing *Childress v. Taylor*, 945 F.2d 500, 507 (2d Cir. 1991)); see also 2 PATRY ON COPYRIGHT § 5:6 (“Classic examples of interdependent joint authorship include the collaborative musical works of Gilbert and Sullivan, the Gershwin brothers, Rodgers and Hammerstein, and Siegel and Shuster. These works are the result of the interdependent contributions of the collaborators, i.e., one person wrote the lyrics and the other wrote the music, *either of which could on its own as [sic] an independent work*, but which, when combined, form a single ‘interdependent’ joint work.”) (emphasis added). This understanding of the term “interdependent” seems to parallel the pre-1976 term “composite work,” which, as contradistinguished from the term “joint work,” was a work consisting of “matter drawn from various sources or contributed by different authors,” or made up of “parts which are ‘clearly discrete and readily capable of being used or are ‘intended to be used separately and whose only unity is that they are bound together.’” See Alfred H. Wasserstrom, *Copyrighting of Contributions to Composite Works: Some Attendant Problems*, 31 NOTRE DAME L. REV. 381, 391–92 n.57 (1956) (quoting ARTHUR WEIL, *AMERICAN COPYRIGHT LAW* 116 (1917)).

133. See 2 PATRY ON COPYRIGHT § 5:6 (“By contrast, examples of an inseparable joint work include two or more individuals collaboratively writing a screenplay, or a work of visual art. In these cases, the collaborators’ contributions are woven into a whole, and *the individual contributions cannot be separated into different works.*”) (emphasis added).

134. See, e.g., *Gaiman v. McFarlane*, 360 F.3d 644, 659 (7th Cir. 2004) (“One professor has brilliant ideas but can’t write; another is an excellent writer, but his ideas are commonplace. So they collaborate on an academic article, one contributing the ideas, which are not copyrightable, and the other the prose envelope, and . . . they sign as coauthors. Their intent to be the joint owners of the copyright in the article would be plain, and that should be enough to constitute them joint authors within the meaning of 17 U.S.C. § 201(a).”) (citing 1 NIMMER ON COPYRIGHT § 6.07).

that [her contribution] would be merged with the contributions of other authors.”¹³⁵ Congress may have enunciated the latter category to accommodate co-authors who do not actively collaborate but who nonetheless merge “interdependent,” effectively free-standing works into a “unitary whole,” such as the screenplay and sound track of a motion picture or the music and lyrics that make up a song¹³⁶ (though real life examples in fact suggest close collaboration between composers and lyricists).¹³⁷

The “interdependent” variety of joint works may arise either from collaboration between co-authors,¹³⁸ or if “each of the authors prepared his or her contribution with the knowledge and intention that it would be merged with the contributions of other authors.”¹³⁹ The “inseparable” variety of joint works, however, implies collaboration. It is difficult to imagine how the contributions could be indistinguishable (and thus constitute “inseparable” parts of a “unitary whole”) without the contributors working together in active collaboration. Co-authors need not work together physically,¹⁴⁰ but in order to render the contributions “inseparable” it would seem that co-authors must, at the time of each individual’s creation, be aware of each other’s specific

135. “Under the definition of section 101, a work is ‘joint’ if the authors collaborated with each other, or if each of the authors prepared his or her contribution with the knowledge and intention that it would be merged with the contributions of other authors as ‘inseparable or interdependent parts of a unitary whole.’” See S. REP. NO. 94-473, *supra* note 130, at 103–04; H.R. REP. NO. 94-1476, *supra* note 130, at 120.

136. The legislative history lists songs, operas, and motion pictures as examples of interdependent joint works. See H.R. REP. NO. 94-1476, *supra* note 130, at 120; S. REP. NO. 94-473, *supra* note 130, at 103.

137. See Stephen Holden, *Composer And Librettist: The New Chemistry*, N.Y. TIMES, July 27, 1986, <https://www.nytimes.com/1986/07/27/theater/composer-and-librettist-the-new-chemistry.html> [perma.cc/SC3B-FFMB] (describing several famous songwriting duos and their methods of collaboration, and noting that the “age-old question, ‘Which comes first, words or music?’ has three answers . . . either one can come first, or else the songs are pieced together more or less simultaneously”).

138. *Id.* (noting that when Leonard Bernstein and Stephen Sondheim collaborated, “Lenny would develop core motifs[,] . . . and [he and Sondheim] . . . would discuss them and argue the meaning and in that way [they] would grow the songs together”).

139. *Id.* (noting that when Richard Rodgers and Lorenz Hart worked together, “Rodgers would usually play a completed melody,” the two would then “agree[] on a general theme,” and Hart would then “write the words”).

140. See *Baker v. Robert I. Lappin Charitable Found.*, 415 F. Supp. 2d 473, 488 (S.D.N.Y. 2006) (“[T]he law does not require that joint authors work together or in the same place or contribute to every aspect of a project.”); 1 NIMMER ON COPYRIGHT § 6.03 (noting that “joint authorship” does not require “that the several authors must . . . work in physical propinquity, or in concert, nor that the respective contributions made by each joint author must be equal either in quantity or quality”); Holden, *supra* note 137 (noting that Gilbert and Sullivan, “the most renowned of collaborators,” “communicated by mail”).

contributions and work together to “[weave them] into a whole.”¹⁴¹ As Judge Learned Hand indicated, there is no evidence of a “joint design” to create a joint work if the later-added material occasioned no reworking of the underlying text.¹⁴² Co-authors who collaborate reciprocally influence each other’s contributions.

Figure 2: Types of Joint Works and Modes of Co-Authorship

	“if the authors collaborated with each other”	“if each of the authors prepared his or her contribution with the knowledge and intention that it would be merged with the contributions of other authors”
“Inseparable” parts of a unitary whole	<p>e.g. Collaboration between author A (provides the detailed plot) + author B (provides the prose envelope)</p> <p>(see, e.g., <i>Gaiman v. McFarlane</i>, 360 F.3d 644, 659 (7th Cir. 2004))</p>	?
“Interdependent” parts of a unitary whole	<p>e.g. Collaboration between composer and lyricist who “piece[] together their contributions simultaneously”</p> <p>(see, e.g., <i>Leonard Bernheim and Stephen Sondheim</i>)</p>	<p>e.g. Composer writes the melody and arrangement, sends to her lyricist-partner, who then writes the libretto</p> <p>(see, e.g., <i>Richard Rodgers and Lorenz Hart</i>)</p>

2. Contemporaneous “Intent to Merge” and Unacquainted Co-Authors

The legislative history also posits intent to merge as a criterion for both interdependent parts and inseparable parts of the work as a whole,¹⁴³

141. 2 PATRY ON COPYRIGHT § 5:6 (noting that in “inseparable” joint works, “the collaborators’ contributions are woven into a whole, and the individual contributions cannot be separated into different works”).

142. See *Edward B. Marks Music Corp. v. Jerry Vogel Music Co.*, 140 F.2d 266, 267–68 (2d Cir. 1944) (referring to *Harris v. Coca-Cola Co.*, 73 F.2d 370 (5th Cir. 1934)) (rejecting joint works characterization of asynchronous contribution of illustrations to a literary text because the addition of the illustrations brought about “no change in the text”).

143. See *Erickson v. Trinity Theatre, Inc.*, 13 F.3d 1061, 1068–69 (7th Cir. 1994) (noting that while the legislative history may “appear[] to state two alternative criteria—one focusing on the act of collaboration and the other on the parties’ intent,” “the statutory language clearly requires that each author intend that their respective contributions be merged into a unitary whole,” that “[f]ocusing solely upon the fact of contemporaneous input by several parties does not satisfy the statutory requirement that the parties intend to merge their contributions into

emphasizing that “[t]he touchstone here is intention, at the time the writing is done, that the parts be absorbed or combined into an integrated unit.”¹⁴⁴ The House and Senate Reports appear to envision simultaneous intent to merge contributions, and by implication some interaction among putative co-authors.¹⁴⁵ After all, how else could the contributors have the “knowledge” that their parts would be merged?

However, some commentators contend that “intent to merge” requires neither actual collaboration nor even knowledge of one’s putative co-author.¹⁴⁶ In support of this view, one might argue that the statute requires only contemporaneous intent to merge inseparable contributions, so that, in our short-story hypothetical,¹⁴⁷ the initiating author might create her portion with the intention that later-comers whom she will never meet will merge their contributions. The serial contributors, albeit not necessarily working with each other, are working with each participant’s contributions. Arguably, the initiating author’s ignorance of who would write the chosen ending, or of how the ending would unfold, need not exclude the initiator from sharing co-authorship status with all the other contributors.

But this scenario seems to collapse the distinction between joint works and derivative works, a distinction the legislative history seeks to maintain.¹⁴⁸

a unified work,” and that collaboration alone, absent mutual intent to merge contributions, is insufficient to form a joint work).

144. H.R. REP. NO. 94-1476, at 120 (1976); S. REP. NO. 94-473, at 103 (1975).

145. See Ginsburg, *supra* note 127, at 1471 (“[T]he legislative history suggests that, while the co-authors need not actually meet and work together, they must not only intend, but must also be *aware of each other’s contributions*. For there to be not only an ‘intention [] at the time the writing is done’ to combine the parts, but also the knowledge (or at least the reasonable expectation) that the contributions will be merged, it would seem that each contributor’s intent must be fairly contemporaneous.”) (emphasis added); 2 PATRY ON COPYRIGHT § 5:20 (citing, *inter alia*, Marks, 140 F.2d 266) (noting that the “emphasis on intent at the time of creation is attributable to Congress’s desire to depart” from pre-1976 case law holding that “where complementary efforts were performed at different times by authors unacquainted with one another, their product was a joint work . . .”).

146. See 1 NIMMER ON COPYRIGHT § 6.03 (2017) (“[J]oint authorship occurs even though the joint authors do not work together in their common design, do not make their respective contributions during the same period, and indeed even if they are complete strangers to each other.”); see also Shyamkrishna Balganesh, *Unplanned Coauthorship*, 100 VA. L. REV. 1683, 1687–88 (2014) (noting the “extensive variation” in courts’ analysis of the term “intention” in the 17 U.S.C. § 101 definition of “joint work,” and that some courts require only “intent to create a joint work”).

147. See *supra* note 127 and accompanying text (describing the short-story hypothetical).

148. H.R. REP. NO. 94-1476, *supra* note 144, at 120; S. REP. NO. 94-473, *supra* note 144, at 104 (“[A]lthough a novelist, playwright, or songwriter may write a work with the hope or expectation that it will be used in a motion picture, this is clearly a case of separate or

Rather than characterizing the evolving story¹⁴⁹ as a “unitary whole,” it may be more accurate to view it as an underlying work (the initiator’s contribution) and a series of derivative works that “recast, transform[] or adapt[]”¹⁵⁰ the beginning by supplying endings. Moreover, this scenario stretches the temporal limitation we perceive in the House Report. Indeed, under this view, the statutory standard could even encompass unacquainted sequential contributors, for each intends, “at the time the writing [of each individual contribution] is done,” to merge their parts into an integrated unit, even without any specific knowledge of the other contribution with which her work will be merged.¹⁵¹

The capaciousness of “joint works” thus depends on whether the statute in fact allows for something less than active collaboration, among contributors who are strangers to each other, and who are separated in time. To understand why the 1976 Act intended contemporaneous participation, the next subsection reviews the case law under the prior Copyright Act, to which the 1976 Act responded.

3. *Why Congress Required Contemporaneous Intent to Merge Contributions*

Judicially elaborated co-authorship doctrine under the 1909 Act allowed co-authorship status to extend to participants who neither actively collaborated nor were even aware of each other.¹⁵² This approach departed from the English common law norm articulated in *Levy v. Rutley*,¹⁵³ which established that “co-authorship required a predetermined intent to create one integral work on the part of two or more *acquainted* persons working at

independent authorship In this case, the motion picture is a derivative work . . . and section 103 makes plain that copyright in a derivative work is independent of, and does not enlarge the scope of rights in, any pre-existing material incorporated in it.”)

149. See *supra* note 127 and accompanying text (describing the short-story hypothetical).

150. See 17 U.S.C. § 101 (2018) (definition of a derivative work).

151. See *supra* note 145.

152. See, e.g., *Shapiro, Bernstein & Co. v. Jerry Vogel Music Co.*, 221 F.2d 569 (2d Cir. 1955) (holding that the song lyrics written by the appellant were part of a “joint” work rather than a “composite” one); *Edward B. Marks Music Corp. v. Jerry Vogel Music Co.*, 140 F.2d 266 (2d Cir. 1944) (holding that the lyrics written by the defendant and the music written by the plaintiff combined to create a joint work, consequently preserving the constructive trust between the two).

153. *Levy v. Rutley*, (1871) LR 6 C.P. 523 (Eng.).

approximately the same time.”¹⁵⁴ In *Edward B. Marks v. Jerry Vogel Music Co.*,¹⁵⁵ Marks “composed the words for a song . . . which he took to a publisher . . . who bought it.”¹⁵⁶ The publisher then “engaged one Loraine [a composer] to compose music for the words.”¹⁵⁷ The lyricist and the composer “never met until years later, and had not therefore worked in conjunction, except that Marks intended the words to be set to music which someone else should compose” and that Loraine (the composer) “understood that he was composing music for those particular words.”¹⁵⁸ The first-in-time lyricist then “applied for a renewal of the copyright upon the song as a ‘musical composition’ ” (a category which includes music with accompanying lyrics).¹⁵⁹ “[I]f the song was the joint work of Marks and Loraine, when Marks took out the renewed copyright, it was valid, but he held it upon a constructive trust for Loraine.”¹⁶⁰ Judge Learned Hand held that the work was a “joint work” because both the composer and the lyricist created their components “in furtherance of a common design.”¹⁶¹ He noted that “it makes no difference whether the authors work in concert, or even whether they know each other; it is enough that they mean their contributions to be complementary in the sense that they are to be embodied in a single work to be performed as such.”¹⁶²

154. See Note, *Accountability Among Co-owners of Statutory Copyright*, 72 HARV. L. REV. 1550, 1551 (1959) (emphasis added) (observing that “American decisions have substantially modified this intent requirement”). In the case, Levy was the proprietor of a theatre, who had employed a dramatist (Wilks) to write a play. See Elena Cooper, *Joint Authorship In Comparative Perspective: Levy v. Rutley And Divergence Between The UK and USA*, 62 J. COPYRIGHT SOC’Y U.S.A. 245, 255 (2015). After Wilks presented the finished play to Levy, Levy made changes to the dialogue and wrote a new scene without Wilks’s participation. See *id.* at 255–56. After Wilks died, Levy sued a rival theatre which had mounted the play, claiming that he was Wilks’ coauthor. See *id.* at 256.

155. See *Marks*, 140 F.2d 266.

156. *Id.* at 266.

157. *Id.*

158. *Id.*

159. *Id.* at 267.

160. *Id.*

161. *Id.* (“It is true that each knew that his part could be used separately; the words, as a ‘lyric’; the melody, as music. But that was not their purpose; the words and the music were to be enjoyed and performed together; unlike the parts of a ‘composite work,’ each of which is intended to be used separately, and whose only unity is that they are bound together. . . . [But] when both plan an undivided whole . . . their separate interests will be as inextricably involved, as are the threads out of which they have woven the seamless fabric of the work.”).

162. *Id.*; see *Accountability Among Co-owners*, *supra* note 154, at 1551 (noting that Marks established that “not only is an intent at the time of creation to combine with a *particular* person unnecessary to enable that person to be the co-author of the product of a subsequent combination, but even the specific intent at that time to combine with someone else does not prevent it”) (emphasis added).

The Second Circuit further expanded this capacious concept of co-authorship in *Bernstein v. Jerry Vogel Music Co. (12th Street Rag case)*,¹⁶³ holding the contested musical composition a joint work even when the first author never intended for his work to be merged with the contribution of a follow-on author. In that case, a composer wrote “an instrumental piano solo” and then “by assignment transferred all his rights in the piece” to a publisher, who then employed a lyricist to supply lyrics. The publisher registered a copyright in the completed song.¹⁶⁴ Even though the first author created a stand-alone wordless musical composition, the court found the requisite collaborative intent in the publisher, who had succeeded to the composer’s copyright interest. Because the publisher “consent[ed] . . . at the time of the collaboration, to the collaboration by the second author,” the work was joint.¹⁶⁵

The 1976 Act rejected this case law and substituted a requirement of contemporaneous collaboration or intent to merge contributions. While the legislative history emphasized that “[t]he touchstone here is the intention, *at the time the writing is done*, that the parts be absorbed or combined into an integrated unit,”¹⁶⁶ some argue that a requirement of contemporaneous intent does not necessarily imply a full return to the *Levy v. Rutley* rule that the contributors must be acquainted.¹⁶⁷ In other words, if Congress clearly repudiated the *12th Street Rag* case, it may nonetheless have left room to argue for the survival of *Edward B. Marks Music Corp. v. Jerry Vogel Music Co.*¹⁶⁸

163. *Shapiro, Bernstein & Co. v. Jerry Vogel Music Co.*, 221 F.2d 569, 569–70 (2d Cir. 1955).

164. *Id.* at 570.

165. *Id.* (“Since [the assignee’s] intent was to merge the two contributions into a single work to be performed as a unit . . . we should consider the result ‘joint’ rather than ‘composite.’”).

166. H.R. REP. NO. 94-1476, at 120 (1976); S. REP. NO. 94-473, at 103 (1975) (emphasis added); *see also* 2 PATRY ON COPYRIGHT § 5:20 (“Th[e] emphasis on intent at the time of creation is attributable to Congress’s desire to depart markedly from opinions of the Second Circuit [including the *Marks* and *12th Street Rag* cases] [which] held that where complementary efforts were performed at different times by authors unacquainted with one another, their product was a joint work because they had a common design.”).

167. *See* 1 NIMMER ON COPYRIGHT § 6.03 (2017).

168. The legislative history may be in tension with this speculation. The House Report states that to “write a work with the hope or expectation” that it will be incorporated into a motion picture does not make a subsequently incorporated work one of joint authorship with the motion picture. H.R. REP. NO. 94-1476, *supra* note 166, at 120. On the other hand, if “the basic intention behind the writing of the work was for motion picture use,” perhaps a joint work would result. S. REP. NO. 94-473, *supra* note 166, at 104.

Whether courts should entertain that argument turns on the policies one can infer from Congress' discrediting of the Second Circuit's pre-1976 case law. The *Marks* and *12th Street Rag* scenarios both involved the assertion of copyright by the successors in title to the author of a preexisting work (in *Marks*, the poem, in *12th Street Rag*, the musical composition) over a work that combined those works with newly-created, purpose-built complements (in *Marks*, the music, in *12th Street Rag*, the lyrics). In both cases, the combined components formed "interdependent" units. While the facts of each case may have made a finding of joint authorship appear the most equitable outcome,¹⁶⁹ the holdings unmoored from their facts risk producing problematic results. Within the context of "interdependent" joint works, finding co-authorship without acquaintance or contemporaneous intent would effectively allow a later author to bootstrap another's work,¹⁷⁰ and thus to exercise non-exclusive rights in the combined work or in its components, including a component the second author did not create.¹⁷¹ By the same token, because all co-authors must agree to grant exclusive rights,¹⁷² the later author could prevent the first author from transferring exclusive rights in the whole or any of its parts, including the part for which she initially was the sole author. By contrast, recognizing the components as independent works would not have deprived either creator of copyright; the separate works would instead be treated as an original work and a derivative work,¹⁷³ or as two separate copyrightable works joined together as

169. Without a finding of joint authorship, the component works might otherwise have fallen into the public domain for incomplete renewal. See *Edward B. Marks Music Corp. v. Jerry Vogel Music Co.*, 42 F. Supp. 859, 867-68 (S.D.N.Y. 1942) (noting Marks's argument that its renewal copyright "covered only the lyrics" of the song, and the music "entered the public domain" because Loraine "was alive during the last year of the original . . . term and did not make application for a renewal copyright in the music").

170. Courts have shown a consistent concern for protecting "dominant authors" against pesky idea-bearing interlopers who attempt to bootstrap ownership of the dominant author's work. See, e.g., *Childress v. Taylor*, 945 F.2d 500, 507 (2d Cir. 1991) (noting a concern about "spurious claims by those who might otherwise try to share the fruits of the efforts of a sole author of a copyrightable work"); *Erickson v. Trinity Theatre, Inc.*, 13 F.3d 1061, 1063, 1072 (7th Cir. 1994) (denying the co-authorship claim of an actor in a theatre company who claimed that "many decisions about what was to be included [in the work] were made during rehearsals" and noting that the actor's mere suggestion "that [the primary author] include a passage from Macbeth and an introduction to the play does make him a joint author").

171. See *Edward B. Marks Music Corp. v. Jerry Vogel Music Co.*, 140 F.2d 266, 267 (2d Cir. 1944); see also H.R. REP. NO. 94-1476, *supra* note 166, at 120.

172. *Davis v. Blige*, 505 F.3d 90, 101 (2d Cir. 2007) ("[A] co-owner cannot unilaterally grant an exclusive license."); 1 NIMMER ON COPYRIGHT § 6.11 (noting prohibition on one co-owner granting an exclusive license without consent of other co-owners).

173. 2 PATRY ON COPYRIGHT § 5:20 (noting that "under the 1976 Act, [the works produced by the second authors in the *Marks* and *12th Street Rag* cases] would be treated as

a “composite work.”¹⁷⁴ One may therefore infer congressional intent to return to the acquainted co-authors rule of *Levy v. Rutley* when the contributions to the alleged joint work could stand on their own but together form an interdependent whole. The next Section considers whether the same legislative intent extends to “inseparable” joint works.

a) Merger of Inseparable Contributions Without Collaboration?

The logic behind the 1976 Act revisions applies most aptly to *interdependent* works created non-collaboratively, where the contributions to the resulting work can be separated into distinct (copyrightable) components. At least at the time of the 1976 Act’s passage, the only conceivable “inseparable” works arose from active collaboration between putative co-authors.¹⁷⁵ There do not appear

derivative works”); H.R. REP. NO. 94-1476, *supra* note 166, at 120 (characterizing a motion picture that incorporates preexisting elements as a “derivative work”).

174. Neither the 1909 Copyright Act nor the 1976 Act defined the term “composite work” but both acts referred to the term. See Copyright Act of 1909 §§ 3, 4, 23, 24 (mentioning, without defining, “composite works”); § 3 (“The copyright upon composite works or periodicals shall give to the proprietor thereof all the rights in respect thereto which he would have if each part were individually copyrighted under this Act.”); 17 U.S.C. § 304 (2018) (referring to “periodical, cyclopedic, or other composite work”). Commentators note that, under the 1976 Act, the term “encompasses works such as periodicals and encyclopedias that embody contributions from several different authors,” but before 1976 the term was more broadly understood to mean all works composed of parts which are “clearly discrete and readily capable of being used or are ‘intended to be used separately and whose only unity is that they are bound together.’” See GOLDSTEIN ON COPYRIGHT, § 6.3.2(b) (2005); Alfred H. Wasserstrom, *Copyrighting of Contributions to Composite Works: Some Attendant Problems*, 31 NOTRE DAME L. REV. 381, 391–92 n.57 (1956).

175. Judge Posner may have supplied one applicable hypothetical, albeit for the purpose of demonstrating that where the participants do intend to collaborate, it should not be necessary that their uncombined contributions have been separately copyrightable, so long as the combination results in an original work of authorship:

The contents of a comic book are typically the joint work of four artists—the writer, the penciler who creates the art work . . . , the inker . . . who makes a black and white plate of the art work, and the colorist who colors it. The finished product is copyrightable, yet one can imagine cases in which none of the separate contributions of the four collaborating artists would be. The writer might have contributed merely a stock character (not copyrightable, . . .) that achieved the distinctiveness required for copyrightability only by the combined contributions of the penciler, the inker, and the colorist, with each contributing too little to have by his contribution alone carried the stock character over the line into copyright land.

Gaiman v. McFarlane, 360 F.3d 644, 659 (7th Cir. 2004). But if the contributors did not collaborate—for example, if Judge Posner’s writer, penciler, inker, and colorist, each furnished his or her contribution at different times and unbeknownst to each other—there would be no joint work because the participants are not acquainted with one another, and no individual

to be any 1909 Act cases involving asynchronous contributions to an “inseparable” joint work. The dearth of examples makes sense: as discussed above, it is difficult to envision how two or more contributors could interweave elements, none of which separately constitute copyrightable expression, without actively collaborating.¹⁷⁶ Congress therefore did not need to consider the ramifications of requiring that co-authors of an “inseparable” work evince contemporaneous intent to merge their contributions with the specific contributions of their co-authors: the existence of collaboration implies that the co-authors knew of each other’s individual contributions to the “joint design” and contemporaneously intended to merge their contributions into an inseparable whole.¹⁷⁷

Section IV.B argues that the introduction of the generative machine (through which the machine’s designer and the machine’s user can each supply non-copyrightable contributions through their code or instructions, without necessarily collaborating with each other) may realize the previously nonexistent possibility of non-collaboratively created “inseparable” works. Without genuine collaboration between the machine’s designer and its user,¹⁷⁸ the 1976 Act’s requirement of contemporaneous intent to merge specific contributions may deny joint work status to the outputs of such machines unless the machine’s designer had knowledge of the specific contribution supplied by the machine’s user. And because in many cases the individual contributions of designer and user may be insufficient to justify a claim of sole authorship,¹⁷⁹ the denial of joint work status to these outputs would leave them “authorless.”

works of authorship either. Assuming, of course, that the individual contributions of the penciler, inker, and colorist would not qualify as derivative works of which each creator retains sole authorship, the combined product and its components would all be “authorless.”

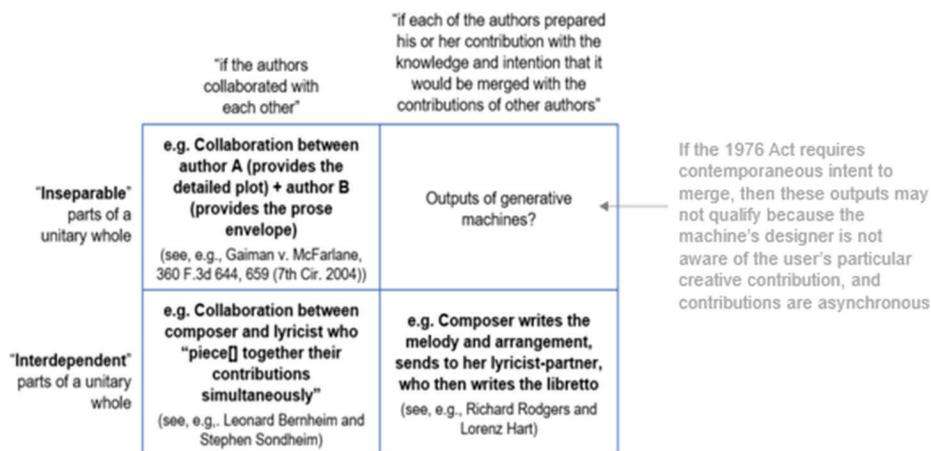
176. See *supra* notes 132–134 and accompanying text.

177. *MacNeill v. Yates*, 2010 U.S. Dist. LEXIS 57731, at *8 (M.D. Fla. 2010) (“[A]uthors who collaborate must also do so with the requisite intent to combine their efforts — although it is hard to imagine collaborators who would not possess such an intent.”) (quoting H.R. REP. NO. 94-1476, at 120 (1976)).

178. In some instances, the machine’s designers and users collaborate with each other and therefore generate a traditional “inseparable” joint work. See *infra* note 213 (describing the “Next Rembrandt” project).

179. See *infra* Section IV.A (describing the class of “authorless” outputs).

Figure 3: Computer-enabled outputs as non-collaboratively produced “inseparable” works?



b) The Implications of Collaboration Between Co-Authors

By contrast, if the initiator of our hypothetical short story¹⁸⁰ and an invited successor had in fact collaborated, so that they worked together on the ending, and revised the beginning in light of the ending, their finished story would be a classic “inseparable contributions” joint work. If collaboration is a necessary condition to the creation of an inseparable joint work,¹⁸¹ is it also a sufficient condition? Or does the law also pose requirements as to the nature of each collaborator’s contribution? What if the initiator prompted her collaborator: “Let’s write a story about a sheep.” They talk it through; the initiator, never much of a literary stylist, contributing key plot ideas, and the collaborator fleshing out the ideas in splendid prose.¹⁸² Both intend to produce a joint work, but the initiator’s ideas, without her collaborator’s “prose envelope,” would not qualify as a work of authorship. If the contributors have intended to collaborate, or at least contemporaneously strive toward a common design (i.e., creative plan) and reciprocally influence each other’s contributions, the statute does not clearly require that each input justify a stand-alone copyright.

180. See *supra* note 127 and accompanying text.

181. At least in the “analog” context. See *infra* notes 341–344 (suggesting that the outputs of partially-generative machines could be non-collaboratively produced “inseparable” joint works).

182. See *Gaiman v. McFarlane*, 360 F.3d 644, 659 (7th Cir. 2004), discussed *supra* note 134.

Collaborating co-authors “labor together to unite ideas with form”;¹⁸³ the statute’s provision for “inseparable” parts implies that each collaborator may situate anywhere along the broad spectrum from ideas to expression so long as the combined result yields an original work of authorship. The statutory definition¹⁸⁴ does not imply that the contributors must have been ‘authors’ of original works before commencing their collaboration; if the result of their intermingled efforts is an original work of authorship, then the contributors are ‘authors’ of the whole.

Case law, particularly in the Second Circuit, however, has glossed the statutory definition to require that each contribution be independently copyrightable,¹⁸⁵ at least where one party, usually the “dominant author,”¹⁸⁶ disclaims intent to collaborate. A requirement of independent copyrightability may make sense with respect to interdependent contributions, but conflicts with the statute’s express recognition that contributions may be inseparable. It may make more sense to characterize the Second Circuit’s standard as meaning only that “the coauthor’s contribution must be the product of authorship, i.e., expression,”¹⁸⁷ rather than that “a coauthor . . . must be able to obtain a copyright on his or her separate contribution.”¹⁸⁸ So understood, were the Little Prince’s participation in a work’s elaboration limited to “Draw me a sheep!”¹⁸⁹ he would not be a co-author because his command constitutes an

183. 1 NIMMER ON COPYRIGHT § 6.07 (2017).

184. 17 U.S.C. § 101 (2018) (defining “joint work” as “a work prepared by two or more authors with the intention that their contributions be merged into inseparable or interdependent parts of a unitary whole”).

185. *See, e.g.*, *Childress v. Taylor*, 945 F.2d 500, 507 (2d Cir. 1991) (“It seems more consistent with the spirit of copyright law to oblige all joint authors to make copyrightable contributions.”); 2 PATRY ON COPYRIGHT § 5:16 (providing several examples of district court opinions from the Second and Ninth Circuits holding that independently copyrightable contributions are required).

186. 16 *Casa Duse, LLC v. Merkin*, 791 F.3d 247, 261 (2d Cir. 2015).

187. *Huurman v. Foster*, 2010 U.S. Dist. LEXIS 61454, at *12 (S.D.N.Y. June 21, 2010) (“[T]he author must provide more than merely an idea for the joint work, as it is well-established that ‘a copyright does not protect an idea, but only the expression of an idea.’”) (quoting *Kregos v. Associated Press*, 3 F.3d 656, 663 (2d Cir. 1993)).

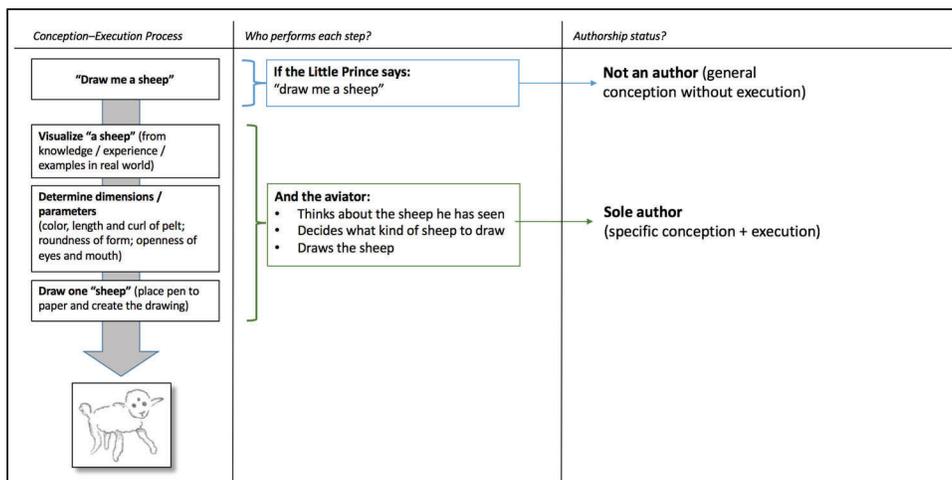
188. Patry argues that courts have misread *Childress*, which actually stood for the basic proposition that each coauthor must contribute some protectable expression: “By ‘copyrightable’ Judge Newman meant only to say that the coauthor’s contribution must be the product of authorship, i.e., expression. He did not mean that in order to be a coauthor one must be able to obtain a copyright on his or her separate contribution.” 2 PATRY ON COPYRIGHT § 5:15; *see* Justin Hughes, *Actors as Authors in American Copyright Law*, forthcoming B.U.L. REV. (citing 2 PATRY ON COPYRIGHT § 5:15). *C.f.* sources cited *supra* note 146.

189. *See supra* note 14.

idea rather than an expression.¹⁹⁰ But were the Little Prince to further develop the idea into an expression by virtue of working together with the aviator, then the intermingling of ideas and form should make both joint authors of the whole.¹⁹¹

Before applying these principles to the world of computer-enabled outputs, we summarize our analysis of traditional principles through the following charts.

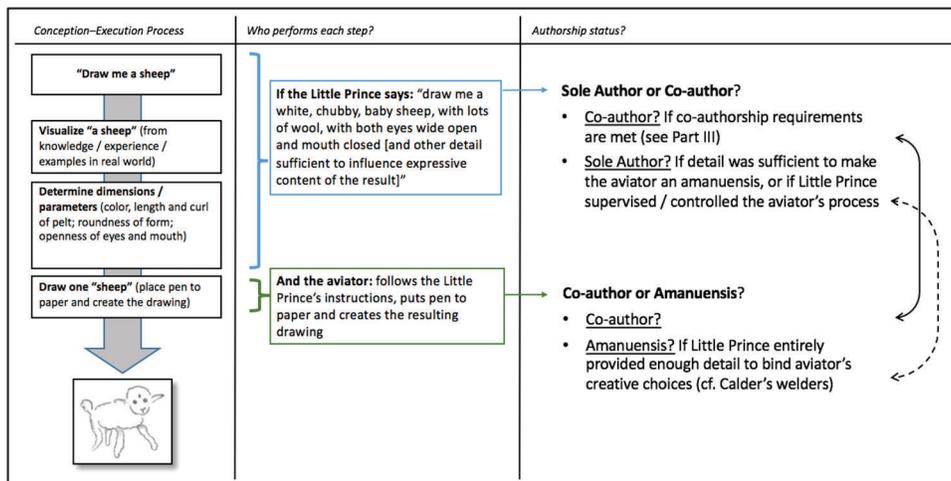
Figure 4: “Draw Me A Sheep” (Example 1, as written by St. Exupéry)



190. See *Latimer v. Roaring Toyz, Inc.*, 550 F. Supp. 2d 1345, 1356–57 (M.D. Fla. 2008) (rejecting a claim of authorship because the putative coauthor, who claimed to be a “collaborator,” had simply provided the primary author with the “idea or concept” for the work, and because his “ideas, conveyed to the author of the copyrighted work, were not copyrightable”).

191. Cf. *Erickson v. Trinity Theatre, Inc.*, 13 F.3d 1061, 1070 (7th Cir. 1994) (noting Nimmer’s “de minimis” view, which posits that if two authors collaborate, with one contributing only uncopyrightable plot ideas and another incorporating those ideas into a completed literary expression, the two authors should be regarded as joint authors of the resulting work, but noting that Nimmer’s view is not “consistent with one of the Act’s premises: ideas and concepts standing alone should not receive protection” and that “contribution of an idea is an exceedingly ambiguous concept”). *Erickson’s* critique of Nimmer fails to recognize that the act of collaboration transforms what might be separately unprotectable components into a copyrightable whole.

Figure 5: “Draw Me A Sheep” (Example 2: If the Little Prince had provided specific instructions)



III. AUTHORSHIP OF COMPUTER-ENABLED OUTPUTS

This Part applies the “analog” principles of authorship identified in Part II to the context of machine-enabled outputs. Section III.A queries whether recent developments in artificial intelligence pose a novel problem for copyright law and for authorship doctrine. It concludes that while computer scientists and artists have made great strides in the field of “computational creativity,” today’s generative machines do not earn the mantle of authorship because they are, at best, “faithful agents” of the humans who interact with them. Thus, generative machines should be examined through the lens of copyright’s previous treatment of tools and amanuenses, explored previously in Sections II.A and II.B. Section III.B turns to the more appropriate question of how to allocate authorship among the human creators who interact with generative machines. It presents a taxonomy of generative machines: from ordinary tools, to partially-generative machines, to fully-generative machines, and investigates the authorship implications of each category. Because the attribution of authorship in the context of partially-generative machines is the least clear, Section III.C provides a deeper investigation of partially-generative machines and addresses how the conception-plus-execution model of authorship (presented in Part II) applies to the different human participants who interact with these machines.

A. THE PROBLEM(?) OF ARTIFICIAL INTELLIGENCE

1. *The Wrong Question: Machine “Authorship”*

The Elephant is the most intelligent of animals because he does exactly what we tell him to’ wrote the great American humorist, Will Cuppy. And there are many philosophers and workers in the field of Artificial Intelligence who have talked themselves into a position from which they can no longer see the cutting edge of the joke.¹⁹²

Recent developments in the field of artificial intelligence have stimulated public excitement about the technology’s potential. Artificial intelligence, defined as the “science of programming cognitive abilities into machines,”¹⁹³ may be “the new electricity”¹⁹⁴—a technological development that will have a “transformational impact” on almost every aspect of human activity.¹⁹⁵ Various forms of artificial intelligence increasingly pervade our homes,¹⁹⁶ our businesses,¹⁹⁷ our governments,¹⁹⁸ and our social lives.¹⁹⁹ Surprising

192. Guy Robinson, *Book Review, Artificial Intelligence and Natural Man by Margaret A. Boden*, 54 PHIL. 130, 130 (1979).

193. *Why AI Is the ‘New Electricity’*, KNOWLEDGE@WHARTON (Nov. 7, 2017), <http://knowledge.wharton.upenn.edu/article/ai-new-electricity/> [perma.cc/B8LR-LPF5].

194. *Id.*

195. *Id.* (“AI has advanced to the point where it has the power to transform every major sector in coming years.”).

196. *See OK, House, Get Smart: Make the Most of Your AI Home Minions*, WIRED, May 16, 2017, <https://www.wired.com/2017/06/guide-to-ai-artificial-intelligence-at-home/> [perma.cc/J8KY-3DC3] (“If you’re not already having conversations with a cylindrical speaker sitting on the kitchen counter, you will be soon. AI-powered devices like Amazon Echo and Google Home are poised to invade tens of millions more households this year.”).

197. *See* Erik Brynjolfsson & Andrew McAfee, *The Business of Artificial Intelligence*, HARV. BUS. REV., July 2017, <https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence> [perma.cc/BP58-9Q4M] (describing “artificial intelligence, particularly machine learning” as “[t]he most important general-purpose technology of our era” and noting that “[i]n the sphere of business, AI is poised [to] have a transformational impact” on “manufacturing, retailing, transportation, finance, health care, law, advertising, insurance, entertainment, education, and virtually every other industry”).

198. *See* Cary Conglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEORGETOWN L.J. 1147, 1151–53 (2017) (noting “[m]achine learning uses by defense, homeland security, and criminal law enforcement authorities,” and arguing that “many aspects of public administration could undoubtedly benefit from the application of machine-learning algorithms”).

199. *How Artificial Intelligence Is Edging Its Way Into Our Lives*, N.Y. TIMES, Feb. 12, 2018, <https://www.nytimes.com/2018/02/12/technology/artificial-intelligence-new-work-summit.html> [perma.cc/XFM6-Z8KX] (noting how Facebook is “applying artificial intelligence to ward off bad actors and keep its platform free of toxicity” by using “image classifier algorithms that find and automatically remove nude photos and videos” from the social network); James Jackson, *How a Matchmaking AI Conquered (and Was Exiled) from Tinder*,

accomplishments by artificially intelligent machines, like the defeat of the world's best Go player,²⁰⁰ or the creation of a new conversational language between experimental chat bots,²⁰¹ have led us to anticipate the advent of what was once the stuff of science fiction: the thinking machine.²⁰² But there is ample cause for skepticism: rapid advancements in artificial intelligence do not necessarily signal the coming of robots capable of replacing human ingenuity, creativity, or innovation.²⁰³ Despite impressive developments in practical artificial intelligence (artificial intelligence designed for a narrow specific purpose, like business analytics, language translation, etc.), the idea of true machine thought, guided by the sort of “intrinsic motivation” that drives all human behavior, may still be far off.²⁰⁴

VICE: MOTHERBOARD (Nov. 6, 2017), https://motherboard.vice.com/en_us/article/8x5vqx/how-a-matchmaking-ai-conquered-and-was-exiled-from-tinder [perma.cc/S599-VLAG] (describing the use of “AI and deep learning programs to . . . play matchmaker for humans”).

200. Christopher Moyer, *How Google's AlphaGo Beat a Go World Champion*, ATLANTIC, Mar. 28, 2016, <https://www.theatlantic.com/technology/archive/2016/03/the-invisible-opponent/475611/> [perma.cc/AW2A-SYKY] (describing how “the strongest Go player in the world, Lee Sedol” lost a series of Go matches to Google’s AI-powered AlphaGo machine).

201. Tony Bradley, *Facebook AI Creates Its Own Language in Creepy Preview of Our Potential Future*, FORBES, July 31, 2017, <https://www.forbes.com/sites/tonybradley/2017/07/31/facebook-ai-creates-its-own-language-in-creepy-preview-of-our-potential-future/#53d8b5b9292c> [perma.cc/P8E8-CUF4] (“Facebook shut down an artificial intelligence engine after developers discovered that the AI had created its own unique language that humans can’t understand.”).

202. Isaac Asimov, *Robot Dreams*, in ROBOT DREAMS (REMEMBERING TOMORROW) 23, 24 (1986) (describing a robot that uses a “positronic brain pattern remarkably like that of a human brain,” capable of dreaming).

203. Ron Miller, *Artificial Intelligence Is Not As Smart As You (Or Elon Musk) Think*, TECHCRUNCH (July 25, 2017), <https://techcrunch.com/2017/07/25/artificial-intelligence-is-not-as-smart-as-you-or-elon-musk-think/> [perma.cc/BUR8-T7GH] (noting the “there is a tendency for us to assume that if the algorithm can do x, it must be as smart as humans” and that in reality, artificial intelligence is “not really like human intelligence at all”).

204. Jean-Christophe Baillie, *Why AlphaGo Is Not AI*, IEEE SPECTRUM, Mar. 17, 2016, <https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/why-alphago-is-not-ai> [perma.cc/XZT5-J446] (noting that while “the rapid advances of deep learning and the recent success of this kind of AI at games like Go are very good news,” “something similar” to human-like “intrinsic motivation,” the desire to “explore” and “try” which is driven by “some kind of intrinsic curiosity” “is needed inside [an AI] system to drive its desire to . . . structure the information of the world” and “create meaning”); *id.* (noting that in “today’s AI programs” “all the meaning is actually provided by the designer of the application: the AI . . . doesn’t understand what is going on and has a narrow domain of expertise”).

Artificial intelligence, as a concept, as a practical field of computer science, and as a challenge to legal norms, is far from new.²⁰⁵ Since the 1980s, legal commentators have contemplated how intellectual property law might deal with AI,²⁰⁶ and the legal academy has developed a substantial body of commentary on the concept of automated “creativity” and its potential impact on intellectual property rights.²⁰⁷ In the field of copyright law, commentators have hotly debated whether creative machines can be “authors,” and whether the creations of such a “machine author” should be legally protected by existing copyright regimes.²⁰⁸ Examples of “creative machines” abound: programmers have trained algorithms to create news reports,²⁰⁹ musical

205. *Why AI Is the New Electricity*, *supra* note 193 (“[E]ven though there’s a perception that AI was a fairly new development, it has actually been around for decades.”). Alan Turing’s 1950 paper, *Computing Machinery and Intelligence*, famously proposed the question “[c]an machines think?” and proposed a test through which scientists could identify a thinking machine. *See generally* A. M. Turing, *Computing Machinery and Intelligence*, LIX MIND 433 (1950).

206. Pamela Samuelson, *Allocating Ownership Rights in Computer-Generated Works*, 47 U. PITT. L. REV. 1185, 1186–87 (1986) (“As ‘artificial intelligence’ (AI) programs become increasingly sophisticated in their role as the ‘assistants’ of humans in the creation of a wide range of products—from music to architectural plans to computer chip designs to industrial products to chemical formulae—the question of who will own what rights in the ‘output’ of such programs may well become a hotly contested issue.”). The United States Copyright Office first contemplated the concept of computer-generated works in 1965. *See* Miller, *supra* note 25, at 1044–47 (noting that in 1965 the office identified “[t]he crucial question” to be “whether the ‘work’ is basically one of human authorship, . . . or whether the traditional elements of authorship in the work . . . were actually conceived and executed not by a man but by a machine”) (quoting U.S. COPYRIGHT OFF., ANN. REP. REG. COPYRIGHTS 68 at 7 (1966)).

207. *See, e.g.*, Bridy, *supra* note 3; Ralph D. Clifford, *Intellectual Property in the Era of the Creative Computer Program: Will The True Creator Please Stand Up?*, 71 TUL. L. REV. 1675 (1997); Miller, *supra* note 25; Denicola, *supra* note 4; Ryan Abbott, *Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the United Kingdom*, in RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND DIGITAL TECHNOLOGIES (Tanya Aplin, ed.) (forthcoming 2020); James Grimmelman, *There’s No Such Thing as a Computer-Authored Work—And It’s a Good Thing, Too*, 39 COLUM. J.L. & ARTS 403 (2016); Bruce E. Boyden, *Emergent Works*, 39 COLUM. J.L. & ARTS 377 (2016); Andrew J. Wu, *From Video Games to Artificial Intelligence: Assigning Copyright Ownership to Works Generated by Increasingly Sophisticated Computer Programs*, 25 AIPLA Q.J. 131 (1997); Timothy L. Butler, Note, *Can a Computer be an Author? Copyright Aspects of Artificial Intelligence*, 4 HASTINGS COMMUN. & ENT. L.J. 707 (1981).

208. *See, e.g.*, Bridy, *supra* note 3, at 21–27 (considering various definitions of “creativity” and whether machines could ever emulate it); *id.* (assuming that a “generative software program” can be the “author-in-fact” of a copyrighted work, and questioning in whom the law should vest ownership of such a work).

209. *See Robot Writes LA Times Earthquake Breaking News Article*, BBC NEWS (Mar. 18, 2014), <http://www.bbc.com/news/technology-26614051> [perma.cc/YKK9-PQ47] (noting how a programmer “created an algorithm that automatically generates a short article when an earthquake occurs” and can also “generate stories about crime in the city”); Samantha Goldberg, *Robot Writers and the Digital Age*, AM. JOURNALISM REV. (Nov. 25, 2013),

compositions,²¹⁰ entire books,²¹¹ “original” works of visual art,²¹² and works of visual art modeled after the styles of great artists of history.²¹³ Such examples have led many commentators to assume that copyright is entering a “digitally induced crisis” brought on by the coming problem of “AI authorship” and “procedurally generated works”—outputs of generative machines designed to create works and to mimic human creativity.²¹⁴ But the concept of “machine

<http://ajr.org/2013/11/25/computer-might-replace-robot-journalism-digital-age/> [perma.cc/VTQ6-5599] (noting the work of two startups, Narrative Science and Automated Insights, which have “developed sophisticated computer programs that analyze large amounts of data and automatically generate news stories”).

210. A team of programmers in Spain created a computer they call “Iamus” which composes pieces of contemporary classical music in score form, using a set of training data composed of other compositions of the same genre. See Sylvia Smith, *Iamus: Is this the 21st century’s answer to Mozart?*, BBC NEWS (Jan. 3, 2013), <http://www.bbc.com/news/technology-20889644> [perma.cc/W95Q-46JF]. Iamus creates a piece of music at the push of a button—the programmers need only supply the machine with an intended piece duration and instrumentation. *Id.* Other researchers are designing algorithms to create more varied types of music. See Alex Marshall, *From Jingles to Pop Hits, A.I. Is Music to Some Ears*, N.Y. TIMES, Jan. 22, 2017, <https://www.nytimes.com/2017/01/22/arts/music/jukedek-artificial-intelligence-songwriting.html> [perma.cc/VMY6-N8TC] (noting the efforts of Jukedek, an online product which allows users to create unique pieces of music by inputting basic parameters using a neural network trained with musical examples, and charges users \$21.99 to use the outputted track, and similar efforts by Google).

211. A marketing professor at INSEAD has “developed a small arsenal of algorithms capable of automatically generating textbooks, crossword puzzles, poems and books on topics ranging from bookbinding to cataracts.” See Bianca Bosker, *Philip Parker’s Trick for Authoring Over 1 Million Books; Don’t Write*, HUFFINGTON POST (Feb. 11, 2013), https://www.huffingtonpost.com/2013/02/11/philip-parker-books_n_2648820.html [perma.cc/T4M7-S7W2].

212. Harold Cohen developed a painting machine (“AARON”), trained with “lists of object/body elements and the relationships between them” and other fundamental rules of form which it then uses to generate works of “still life and portraits of human figures without photos or other human input” which are not predictable by their programmer. See Richard Moss, *Creative AI: The Robots That Would Be Painters*, NEW ATLAS (Feb. 16, 2015), <https://newatlas.com/creative-ai-algorithmic-art-painting-fool-aaron/36106/> [perma.cc/38E9-R8SH]; Bridy, *supra* note 3, at 24 (noting that “Harold Cohen doesn’t ‘use’ AARON to paint in the same way that he would ‘use’ a paintbrush to paint; AARON paints”).

213. A team at JWT, a marketing agency, created a machine to create the “Next Rembrandt,” a painting in the style of the artist. See Tim Nudd, *Inside ‘The Next Rembrandt’: How JWT Got a Computer to Paint Like the Old Master*, ADWEEK (June 27, 2016), <http://www.adweek.com/brand-marketing/inside-next-rembrandt-how-jwt-got-computer-paint-old-master-172257/> [perma.cc/B4BZ-35ZM]; see also ING Presents: *The Next Rembrandt*, <http://www.nextrembrandt.com> [https://perma.cc/7RS4-RM6V] (last visited Sept. 10, 2019).

214. Bridy, *supra* note 3, at 27.

authorship” reflects what we hope²¹⁵ (or fear)²¹⁶ artificial intelligence will eventually become more than what it is today. Today’s artificial intelligence is “not really like human intelligence at all.”²¹⁷ Even the most sophisticated AI systems are, at their core, convoluted logical labyrinths designed to approximate narrow slices of human intelligence through “brute-force computational strength.”²¹⁸

The idea that a machine could be an “author” of a work must rest on the assumption that a machine is capable of carrying out the required elements of authorship: conception and execution. But today’s machines are fundamentally sets of processes designed by humans to accomplish specific tasks.²¹⁹ Their outputs may appear to be “creative” and may even be aesthetically equivalent to works produced by human authors,²²⁰ but to attribute a work’s expressive

215. See IAIN M. BANKS, *CONSIDER PHLEBAS* (1987) (describing a post-scarcity, utopian society led by highly advanced benevolent artificial intelligence or “Minds”).

216. See Rory Cellan-Jones, *Stephen Hawking Warns Artificial Intelligence Could End Mankind*, BBC NEWS (Dec. 2, 2014), <http://www.bbc.com/news/technology-30290540> [perma.cc/6GCN-HSY5] (“[AI] would take off on its own, and re-design itself at an ever increasing rate . . . Humans, who are limited by slow biological evolution, couldn’t compete, and would be superseded.”) (quoting Professor Stephen Hawking).

217. Miller, *supra* note 203 (“The analogy that the brain is like a computer is a dangerous one, and blocks the progress of AI.”) (quoting Pascal Kaufmann); see also Nick Ismail, *True AI Doesn’t Exist Yet . . . It’s Augmented Intelligence*, INFO. AGE (Sept. 11, 2017), <http://www.information-age.com/true-ai-doesnt-exist-augmented-intelligence-123468452/> [perma.cc/4P9V-6Y5Z] (noting that “[w]hile many companies claim to provide ‘AI-driven’ solutions, in reality they’re leveraging machine learning techniques at best, developing . . . augmented intelligence” and noting that “IBM . . . agrees with this definition, and believes today’s technologies are more data-driven than ever but aren’t yet advanced enough to think for themselves”).

218. Miller, *supra* note 203 (describing the victory of Google’s AlphaGo over Lee Sedol as “more about training algorithms and using brute-force computational strength than any real intelligence,” noting that “training an algorithm to play a difficult strategy game isn’t intelligence, at least as we think about it with humans,” and further noting that Google’s AlphaGo “actually couldn’t do anything else but play Go on a standard 19 x 19 board . . . the AlphaGo team admitted . . . that had there been even a slight change to the size of the board, ‘we would have been dead’”) (quoting Former MIT robotics professor Rodney Brooks).

219. See Bridy, *supra* note 3, at 10, 22 (“An intelligent programmer or team of programmers stands behind every artificially intelligent machine. People create the rules, and machines obediently follow them—doing . . . only whatever we order them to perform, and nothing more.”).

220. *Machine Creativity Beats Some Modern Art*, MIT TECH. REV., June 30, 2017, <https://www.technologyreview.com/s/608195/machine-creativity-beats-some-modern-art/> [perma.cc/DL6S-ZSBT] (describing a test to determine “how humans react to . . . machine-generated art” which tested human-generated Abstract Expressionist paintings against similar paintings generated by a machine, and found that in some cases “viewers had a hard time telling the difference”).

value to the machine that physically generated that work is to indulge in a fiction.²²¹ One should not reason backward from the apparent equivalence of the output to assume equivalence of the creative processes.

Any apparent “creativity” in a machine’s output is directly attributable either to the code written by the programmers who designed and trained the machine, or to the instructions provided by the users who operate the machine. No machine is itself a *source* of creativity. Even if the output of the machine surprises the humans who programmed, trained, or operated the machine by producing an unanticipated output that *appears* to be the result of some unseen creative force, one should not jump to the conclusion that the machine has earned the title of “author.” Every unanticipated machine output arises directly from some human instruction programmed into the machine. The machine’s designer might write a complex web of code that instructs the machine to analyze a data set, “learn” patterns, and then utilize those patterns to create outputs. The designer might also program randomness to vary the machine’s outputs and its processes.²²² But the resulting output, even if unique and completely unpredictable, is the direct result of the machine’s *process*, which, in turn, is inevitably the brainchild of some human developer or user.²²³

Copyright law has already developed a principle to deal with creative exploits that involve the articulation of a detailed creative process by a primary actor, and the fulfillment of that process by a secondary actor. As Section II.B showed, authors may delegate creative tasks to amanuenses without losing their status as sole authors. When those amanuenses act as “faithful agents”—operating under the broad control of and within the scope of the authority delegated by the author-principal—copyright law is content to ignore the contributions of the amanuenses and instead recognize the principal-creator as the sole author. When a principal-author defines tasks for an agent-amanuensis in “specific detail,”²²⁴ exercising a “high degree of control” over

221. See Clifford, *supra* note 207, at 1685–86 (discussing the ill-defined concept of the “author” and concluding that the word is a “term of art” and that “for now” the author of a computer-enabled work “cannot be the computer”).

222. See BEN GOERTZEL, *THE STRUCTURE OF INTELLIGENCE: A NEW MATHEMATICAL MODEL OF MIND* 12 (1993) (a “computer which involves chance as well as the precise following of instructions” is called a “stochastic computer”).

223. Artists have relied on process-based composition since well before the recent fervor over “generative art” and “computational creativity.” See *supra* note 105 (describing process-based art).

224. See *Andrien v. S. Ocean Cty. Chamber of Commerce*, 927 F.2d 132, 135 (3d Cir. 1991).

the process of creation,²²⁵ the principal-author's sole authorship remains undisturbed despite the physical execution of the creative process by the agent. The agent-amanuensis becomes an author in her own right only if she embarks upon a "frolic of [her] own,"²²⁶ acting "entirely without"²²⁷ the influence of the principal-author.

The broader principle behind amanuensis doctrine holds that an agent's acts under the creative control and direction of a principal are the authorial acts of the principal, not of the agent.²²⁸ Today's machines, of course, are incapable of embarking upon "frolics of [their] own."²²⁹ Every action, step, or calculation made by a machine is the product of the precise articulation of commands by a human programmer or machine-operator (including

225. *Lindsay v. The Wrecked and Abandoned Vessel R.M.S. Titanic*, 1999 WL 816163, at *4–5 (S.D.N.Y. Oct. 13, 1999).

226. *Joel v. Morison* [1834] EWHC KB J39 (Eng.).

227. *Geshwind v. Garrick*, 734 F. Supp. 644, 649 (S.D.N.Y. 1990).

228. This principle is distinct from the work-for-hire doctrine, which is constrained in application to employees acting "within the scope of [their] employment" and to persons conducting one of nine statutorily enumerated types of work "specially ordered or commissioned," and which embraces the employer or commissioner of a work completed by another as "a legal fiction." See 17 U.S.C. § 101 (2018); Catherine L. Fisk, *Authors at Work: The Origins of the Work-for-Hire Doctrine*, 15 YALE J.L. & HUMAN. 1, 4 (2003). The agency-law principle behind the amanuensis doctrine, unlike the work-for-hire doctrine, upholds the principal-author's claim as the author-in-fact and the author-in-law—not because of any employment relationship between principal-author and agent-amanuensis, but because of the imputation of the agent-amanuensis's acts to the author-principal.

229. See Ana Ramalho, *Will Robots Rule The (Artistic) World?: A Proposed Model For The Legal Status of Creations by Artificial Intelligence Systems*, 21 J. INTERNET L. 1, 13 (2017) (noting that artificially intelligence machines are not capable of exercising "judgement" or "self-criticism," cannot "imagine things [they have] never seen," and lack "(at least for now) certain intention and content states like belief and desire, which could inform . . . imagination and/or creativity"). Professor Ramalho argues that, as a matter of U.S. copyright law, artificially intelligent machines cannot be authors because they lack the "intention or purpose to create." *Id.* at 6; see also *id.* at 4 (citing *Feist Publ'ns v. Rural Tel. Serv. Co.*, 499 U.S. 340, 346–47 (1991) (noting that an author must prove "those facts of originality, of intellectual protection, of thought, and conception")). We do not endorse the view that authorship requires the putative author to claim that she had the "purpose to create." See Ginsburg, *supra* note 6, at 1085 (arguing against the proposition that "intent to create" or "intent to be an author" is a requirement of authorship). But see David Nimmer, *Copyright in the Dead Sea Scrolls: Authorship and Originality*, 38 HOUS. L. REV. 1, 159, 205 (2001) (noting that "intent is a necessary element of the act of authorship" and that the plaintiff "must intend to author in order for a work of authorship to emerge"). However, we nonetheless conclude that today's machines cannot be considered authors because they act solely by virtue of the precise commands provided by their human programmers or users. See *supra* notes 22–24; BRINGSJORD & FERRUCCI, *supra* note 22, at xxiv ("As we uncover reasons for believing that human creativity is in fact beyond the reach of computation, we will be inspired to nonetheless engineer systems that dodge these reasons and appear to be creative.").

programmed randomness). Machines are, in essence, perfect agents of the humans who design and use them. They require no supervision, because they are by their very nature incapable of deviating from the instructions given to them.²³⁰

This line of reasoning prompts the inevitable question: at what point will a machine be able to be a principal-author in its own right? At what level of technological sophistication will a machine become capable of going off on a “frolic of [its] own” and creating a work “entirely without”²³¹ the instructions of a human programmer?²³² We expect that these questions—which implicate the elusive concepts of “free will” and the underpinnings of human consciousness—will be the subject of a continuing debate well beyond the scope of copyright law.²³³ But for the purposes of this Article, it should suffice to note that today’s machines, and those of foreseeable tomorrows, are entirely subservient to the humans who delineate their instructions and tasks. Rejecting the idea of “machine authorship” requires no novel twists of doctrinal logic: as long as machines follow our instructions, they are incapable of being more than obedient agents in the service of human principals.

230. Innovations in machine-learning and other forms of “artificial intelligence” which have enabled computer scientists to design self-programming and self-modifying code do not change this conclusion. A machine capable of self-modification or self-improvement is simply a set of processes on top of which programmers have designed a set of meta-processes—algorithms which analyze the machine’s processes and find ways to improve them by experimenting with code variations until an optimal set of instructions have been identified. George Dvorsky, *How Artificial Superintelligence Will Give Birth To Itself*, GIZMODO (July 23, 2014) <https://io9.gizmodo.com/how-artificial-superintelligence-will-give-birth-to-its-1609547174> [<https://perma.cc/K6W5-92BW>] (noting the possibility of AI that can “develop[] its internal cognitive functions”).

231. *Geshwind*, 734 F. Supp. at 649.

232. See ITALO CALVINO, *THE USES OF LITERATURE* 13 (Patrick Creagh trans. 1982) (“The true literature machine will be one that itself feels the need to produce disorder, as a reaction against its preceding production of order: a machine that will produce avant-garde work to free its circuits when they are choked by too long a production of classicism.”); see also Denicola, *supra* note 4, at 282–83 (“Perhaps inevitably, some computer-generated works will one day be created at the instigation of the computer itself.”).

233. See generally JUDEA PEARL & DANA MACKENZIE, *THE BOOK OF WHY: THE NEW SCIENCE OF CAUSE AND EFFECT* (2018) (outlining a vision for how artificial intelligence machines could be programmed to “think” through causal reasoning, which would provide them with human-level intelligence); NICK BOSTROM, *SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES* (2015) (arguing that if scientists succeeded in developing human-level artificial intelligent machines, these machines would quickly exceed human levels of cognitive performance and become “superintelligences” with their own “instrumental goals” like self-preservation and cognitive enhancement).

2. *Machine Learning and the “Black Box” Problem*

The development of sophisticated generative machines utilizing machine-learning techniques like “deep learning” does not change this analysis. Modern research in artificial intelligence focuses on creating “learning” machines—machines that develop their “intelligence” and abilities by analyzing vast amounts of data and deriving general principles through which they can improve their ability to accomplish tasks.²³⁴ Developing a “learning” model is a fundamentally different process from developing a “non-learning” or “expert system” machine: learning models are designed to look for patterns in data, to experiment with different procedural pathways, and to derive general pattern-based principles and use those principles to improve their ability to accomplish particular paths. In other words, “the machine essentially programs itself.”²³⁵

Thus, rather than carefully programming a machine to follow defined sets of rules (i.e., look for a particular word, e.g., “sheep” in an input instruction, search for that word in an image database, and then reproduce that image), the programmer of a “learning” model might simply provide a machine with a

234. See Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 886 (2016) (“[M]achine learning tends to create models that are so complex that they become ‘black boxes,’ where even the original programmers of the algorithm have little idea exactly how or why the generated model creates accurate predictions.”). These “learning” techniques depart from other AI techniques sometimes referred to as “expert system” development, through which “machines [are] given voluminous lists of rules, then tasked with drawing conclusions by recombining those rules.” Cliff Kuang, *Can A.I. Be Taught to Explain Itself?*, N.Y. TIMES, Nov. 21, 2017, <https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html> [perma.cc/NG5W-R6BC].

235. Will Knight, *The Dark Secret at the Heart of AI*, MIT TECH. REV., Apr. 11, 2017, <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/> [perma.cc/3QV2-LZQJ] (“Instead of a programmer writing the commands to solve a problem, the program generates its own algorithm based on example data and a desired output. The machine-learning techniques that would later evolve into today’s most powerful AI systems followed the latter path: the machine essentially programs itself.”). Note, however, that while some commentators and tech evangelists claim that these machines “program[] [themselves],” sophisticated machine-learning algorithms are nonetheless carefully designed, rigorously trained, and closely supervised by their programmers. See *id.* For example, the Google programmers who programmed a “deep learning” algorithm to recognize cats in YouTube videos noted that they “never told [the algorithm] during the training, ‘This is a cat’ ” and that the algorithm “basically invented the concept of a cat.” See *Google’s Artificial Brain Learns To Find Cat Videos*, WIRED (June 26, 2012), <https://www.wired.com/2012/06/google-x-neural-network/> [perma.cc/TJS9-YKF6]. However, the programmers carefully designed the algorithm with a variety of advanced machine-learning techniques, and “trained” the algorithm repeatedly in order to achieve the desired result. See Quoc V. Le et al., *Building High-level Features Using Large Scale Unsupervised Learning*, in PROCEEDINGS OF THE 29TH INTERNATIONAL CONFERENCE ON MACHINE LEARNING 507 (John Langford & Joelle Pineau eds., 2012), <https://ai.google/research/pubs/pub38115> [perma.cc/2WWX-E9DP].

“training” dataset and “tune” the machine until it can derive useful patterns from that dataset and determine how to successfully implement them (i.e., provide the machine a dataset with pairs of images and descriptions, prompt the machine to identify patterns between the images and their patterns until the machine derives some general idea of what a “sheep” looks like, and then ask the machine to generate an image of a “sheep” according to that general form). The programmers of these machines often prioritize accuracy over explainability: instead of devising machines with carefully designed processes, they program the machines to develop their own processes and generalizations in ways that quickly become too complex and multi-dimensional for human programmers to comprehend.²³⁶ Thus, the resulting algorithms suffer from what some AI researchers refer to as the “black-box problem”—their models are “so complex” that “even the original programmers of the algorithm have little idea exactly how or why the generated model” can so accurately perform its task.²³⁷

But the use of more sophisticated “learning” models which we may not precisely understand or supervise—as opposed to more heavily programmed and interpretable “expert systems”—does not change our initial conclusion that machines are not “creative.” The only difference between a “learning” machine and a programmed machine is that the “learning” machine is partially self-tuning—it can develop and improve its own internal processes and can thus develop procedures, the precise intricacies of which elude our understanding. But the machine still proceeds through a process fundamentally controlled by its programmers—the programmers determine what the machine should do (“problem definition”), what to include in the model’s “training set” (data collection and cleaning), what the model should look for in its training set (its “input parameters” and its “outcome variables”),

236. See Zachary Chase Lipton, *The Myth of Model Interpretability*, KD NUGGETS (Apr. 2015) <https://www.kdnuggets.com/2015/04/model-interpretability-neural-networks-deep-learning.html> [perma.cc/8FCK-S5EW] (“To get accuracy rivaling other approaches, typically hundreds or thousands of decision trees are combined together in an ensemble. If we want just a single decision tree, this may come at the expense of the model’s accuracy. And even with one tree, if it grows too large, it might cease to be interpretable.”).

237. See Rich, *supra* note 234, at 886 (“[W]hen an algorithm is interpretable, an outside observer can understand what factors the algorithm relies on to make its predictions and how much weight it gives to each factor. Interpretability comes at a cost, however, as an interpretable model is necessarily simpler—and thus often less accurate—than a black box model.”).

how the machine should seek to optimize itself (its “loss function”), and when the machine should spring into action.²³⁸

The “black-box problem” is similarly irrelevant to the authorship question. Machines are tools of their programmers or of their users, and *understanding* or *explainability* is not a prerequisite for authorial control of a tool. Jackson Pollack’s understanding of the forces of gravity and inertia are irrelevant to his ability to claim authorship over his drip paintings. The photographer need not understand how her digital camera transforms photons into digital image files to “control” the camera and thus maintain an authorial claim to her photographs. And Alexander Calder need not fully understand the intricacies of metal welding to claim authorship over his monumental sculptures, even though he requires expert welders to produce them.

Copyright’s long acceptance of the use of tools and amanuenses is the most appropriate lens through which to deal with the potential problems of machine creation. As we have shown, copyright doctrine is content to ignore the generative role of cameras or art workers, and instead to recognize the authorship claims of the human “master minds” who stand behind them. As Pouillet noted almost a century and a half ago, “[t]he human intelligence, even in the domain of art, can produce nothing without material assistance”²³⁹—and a human is no less an author if her “help be a tool, a machine, [or] another’s hand.”²⁴⁰ The operative principle behind the “master mind” concept of authorship is the recognition that an author may “outsource” the processes of execution to a machine or another human and remain the author as long as she maintains primary control of that process—in Pouillet’s words, as long as “it is . . . the thought of the artist which directs the instrument,—which guides and inspires the material means.”²⁴¹ Artificially intelligent machines, therefore, do not usurp human authorship as long as humans sufficiently “control” them. Since we have posited that computers cannot run off on a “frolic of their own,” some humans will wield the requisite control; the question is whether the reins are in the hands of the machine’s designers or its users.

238. For a helpful explanation of the process of using advanced machine learning models, see generally David Lehr & Paul Ohm, *What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653 (2017).

239. Pouillet on Photography, *supra* note 35, at 599.

240. *Id.*

241. See discussion of “master mind” theory, *supra* Sections II.A and II.B; Pouillet on Photography, *supra* note 35, at 599; Grimmelmann, *supra* note 207, at 408 (“If an author, for her own convenience, decides to automate some of the steps by programming a computer, copyright should not look any less generously upon her.”).

B. THE RIGHT QUESTION: SEARCHING FOR THE HUMAN AUTHOR

If machines are not the “authors” of their outputs, then one must ask whether the humans who design and operate those machines are the authors of those outputs. Until the modern era, this question has been straightforward—the human agent responsible for *using* the tool or machine, not the designer of the tool or inventor of the machine, is the author of its output. As Pouillet put it: “though man’s help be a tool, a machine, another’s hand, he does not the less produce a work of art[; the tool] leaves to the artist, to its fullest extent, the labor of the mind.”²⁴²

Humans who use cameras or other tools are clearly the authors of the works which they use those tools to create, both because those humans *control* the tools (“guide[] and inspire[] the material means”) and because those humans use those tools to express their own ideas (“sentiment, mind, taste”—“the apparatus . . . leaves to the artist, to its fullest extent, the labor of the mind”).²⁴³ The contribution of the machine’s designer is a necessary predicate to the creation of the image, and the camera itself accomplishes much of the executional process. But the camera is a perfect tool for its user—the better the camera, the better it is at producing the image that captures what its user seeks to convey.

The introduction of generative machines—machines which themselves produce works, or which substantially aid in the creation of works—challenges this assumption. A *user* of a generative machine is not necessarily the author of the output, especially when the *designer*²⁴⁴ of the machine exercises more

242. Pouillet on Photography, *supra* note 35, at 599. This conception of user as controller/author also appears in the Final Report the National Commission on New Technological Uses of Copyrighted Works (CONTU). See NAT’L COMM’N ON NEW TECH. USES OF COPYRIGHTED WORKS FINAL REPORT 44 (1978) (comparing computers to cameras, typewriters, and other inert tools of creation, and concluding that the author of a computer-generated work is the person who employs the computer). But eight years later, the Congressional Office of Technology Assessment (OTA) explicitly disagreed with CONTU’s conclusion that computer programs were simply “inert tools of creation” and noted that “[i]f machines are in any sense co-creators, the rights of programmers and users of programs may not be easily determined within the present copyright system.” See OFFICE OF TECH. ASSESSMENT, 99TH CONG., INTELLECTUAL PROPERTY RIGHTS IN AN AGE OF ELECTRONICS AND INFORMATION 72 (1986).

243. Pouillet on Photography, *supra* note 35, at 599.

244. “Designer” refers to the individual (or set of individuals) who prepare the machine for use. Thus, the “designer” of a machine could be the individual who builds the machine’s algorithms (in the case of an “expert system”) or the person who trains a generative machine learning model so that it can produce a set of results. In many contexts, the individual responsible for training a machine-learning algorithm will have the most influence on the algorithm’s outputs. See, e.g., Sobel, *supra* note 20, at 48 (“Much as human creators learn from

creative influence over the resulting work than might the designer of an ordinary tool (like a camera). The idea of a generative machine implies that the machine is *more* than a tool through which the user expresses her own ideas. Unlike ordinary tools, whose outputs reflect the creative contributions of their users, the outputs of generative tools may reflect the creative contributions of the tool's designer, or may reflect the intertwined creative contributions of the designer and the user.

The next Sections describe the spectrum of generative machines and lay out three categories of generative machines: “ordinary tools,” “partially-generative machines,” and “fully-generative machines.” “Ordinary tools”—machines which rely solely on the creative contributions of their users, and for which the creative contributions of the machines’ designers are minimal, nonexistent, or not apparent in the resulting work—form one end of the spectrum. “Fully-generative machines”—machines that rely entirely on the creative contributions of their *designers* and do not require any creative choices made by the users (who simply turn the machine on or tell it to “create”)—form the other end of the spectrum. “Partially-generative machines”—machines that combine the creative contributions of both the user and the designer of the tools, those creative contributions being inseparably fused in the resulting work—form the center of the spectrum.²⁴⁵

1. *“Ordinary” Tools: Those Whose Outputs Reflect the Creative Contributions of Their Users*

In one sense, society develops more and more sophisticated tools with the purpose of enabling the users of those tools to do less and less. New technologies help human creators accomplish their goals more quickly or more

the works of their human predecessors, a technology called ‘machine learning’ allows today’s AI to emulate works of human authorship after being provided with many examples. Depending on the data on which it is trained, an AI could learn to generate prose, paintings, motion pictures, musical compositions, and so on.”). Several copyright scholars have focused on copyright-law issues arising from the dependence of modern machine-learning systems on “training data” which include copyrighted material. *See generally id.* (discussing the application of fair use doctrine to the use of copyrighted material to train AI systems); Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence’s Implicit Bias Problem*, 93 WASH. L. REV. 579 (2018) (discussing how copyright may create or promote biased AI systems by preventing programmers from freely using copyrighted material to train their systems).

245. Professor Bruce Boyden proposed a similar spectrum defined by whether the resulting work reflects “fixed inputs” or “the content of the program written by the programmer” or by “progressive inputs” or “the content input by a downstream user of the program.” *See Boyden, supra* note 207, at 383–91. But Boyden takes a different approach to this problem, which would ask whether each putative author conveyed a “meaning or message” apparent in the resulting work. *See id.* at 393–94.

efficiently, or even accomplish otherwise impossible creative outputs. Adobe Photoshop's Content-Aware Patch tool—which allows users to remove unwanted elements from digital images with the click of a button²⁴⁶—saves photographers the painstaking task of airbrushing unwanted elements (or unwanted people) out of otherwise desirable photographs. AutoCAD, a “software application . . . that enables computer-aided design (CAD) and drafting” is widely used by architects, designers, constructional professionals, and artists to “conceptualize ideas, produce designs and drawings” and schematics.²⁴⁷ AutoCAD allows its users to avoid the detailed calculations necessary to drafting designs, which before AutoCAD may have involved “using an old-school drafting desk and a t-square” and “comput[ing] technical calculations with calculators and mathematical tables”—a process which took days or weeks.²⁴⁸

What, then, is the difference between relatively primitive author tools like the pantograph—an “ingenious tool for copying and resizing images” that “dates [back] to at least the 1600's”²⁴⁹—and more sophisticated tools like Photoshop or AutoCAD? To put the question differently: do these tools give us cause to question Pouillet's basic assumption: “though man's help be a tool, a machine, another's hand, he does not the less produce a work of art” when the putative author uses a tool that does *more* than Pouillet could ever have imagined machines capable of doing? While more sophisticated “ordinary” tools may autonomously accomplish tasks that previously required the application of the author's hand (think, for example, of Photoshop's automatic airbrushing feature), this increased role does not mean that the users of these tools no longer “guide[] and inspire[]” them or that the tools do not “leave[] to the artist, . . . the labor of the mind.” It is still the user of the tool who

246. *Content-Aware Patch and Move*, ADOBE HELPX (Feb. 15, 2017), <https://helpx.adobe.com/photoshop/using/content-aware-patch-move.html> [perma.cc/EB3Y-96TE] (“The Patch tool is used to remove unwanted image elements. The Content-Aware option in the Patch tool synthesizes nearby content for seamless blending with the surrounding content.”).

247. Luke Kennedy, *A Brief History of AutoCAD*, SCAN2CAD (Jan. 5, 2014), <https://www.scan2cad.com/tips/autocad-brief-history/> [perma.cc/226S-U7QK].

248. *Id.* AutoCAD has been hailed as the “greatest advance in construction history” and users tout many benefits including calculation error reduction and the enablement of more complex and ambitious design projects. See *CAD - The Greatest Advance in Construction History*, ARCHITECTS' J. (Dec. 5, 2012), <https://www.architectsjournal.co.uk/cad-the-greatest-advance-in-construction-history/1996442.article> [perma.cc/9MBZ-5PQV].

249. Kevin McGuire, *Using the Pantograph*, WOOD NEWS, <https://www.highlandwoodworking.com/woodworking-tips-1104apr/pantograph.html> [perma.cc/JXR8-CHKG] (last visited Apr. 4, 2018).

directs the tool's accomplishment of its task and entirely forms the conception that will determine the expressive content of the result.

2. *Fully-Generative Machines: Those Whose Outputs Reflect the Creative Contributions of Their Designers*

On the other hand, computer scientists also seek to create machines that can create “on their own”—machines designed not to aid the human creator, but to mimic or replace her. These machines are “fully-generative,” or capable of producing individual outputs with only minimal user input.

Harold Cohen, a pioneer in the field of computer-generated art, devised a painting machine (“AARON”), which creates paintings on demand, but without any specific instruction from its creator.²⁵⁰ Cohen programmed AARON with painting techniques that allow the machine to mix paint and apply paint to canvas, and provided AARON with enough knowledge of basic object forms to allow the machine to be able to “paint still life and portraits of human figures without photos or other human input as reference.”²⁵¹ Cohen saw AARON as an extension of himself—he once noted that he wanted to be the “first artist in history to have a posthumous exhibition of new work.”²⁵² The machine is not a tool “in the traditional sense”²⁵³ because AARON creates without Cohen’s guidance (at least, after Cohen has sufficiently programmed

250. See Harold Cohen, *AARON, Colorist: from Expert System to Expert*, AARONSHOME.COM (Oct. 2006), <http://www.aaronshome.com/aaron/publications/urbana-final.doc> [perma.cc/MY5V-9SE8] (“AARON makes most of its images at night, while I’m asleep.”); Ramalho, *supra* note 229, at 3 (2017) (“AARON will create different paintings, but it will not be able to change its style unless it is programmed to do so. It needs to be fed knowledge and experience to be able to produce works. AARON needs to know the things it depicts in its art, which is done through a generative system—a set of abstract rules that specify the anatomy of the human body.”).

251. See Moss, *supra* note 212. More recently, the artist and Stanford researcher Robbie Barrat used generative adversarial neural networks to create a series of “AI-generated nudes”—abstract images of “amorphous masses of flesh” that have been compared to the works of Francis Bacon and William Undermohlen. See Rahel Aima, *Draw Me Like One of Your French AI-Generated Nudes*, RHIZOME (Apr. 18, 2018), <http://rhizome.org/editorial/2018/apr/18/blobs-of-flesh-categorized-as-human/> [perma.cc/W9FD-K6DA] (commenting on Barrat’s work and noting that Barrat does not “modify by hand what [his] AI outputs” and that “Barrat is only willing to alter the instructions and not the output”).

252. Harold Cohen, *Towards a Diaper-Free Autonomy*, AARONSHOME.COM (Aug. 4, 2017), <http://www.aaronshome.com/aaron/publications/index.html> [perma.cc/VH8S-C59C].

253. Bridy, *supra* note 3, at 21 (noting that “generative software [like Harold Cohen’s AARON]” is not “an author’s tool in the traditional sense; unlike a pen or a paintbrush, or even a camera, generative software has a verbal or visual vocabulary of its own and the ability to compose a range of distinct works from that vocabulary by independently applying a system of rules”).

it): AARON creates images by itself, often while Cohen is asleep, and it does not require any instruction as to *what* it should paint²⁵⁴ or what colors it should use.²⁵⁵ Other programmers have developed similar machines designed to generate poetry, short stories, and musical compositions.²⁵⁶

As we have shown, however, the ability of these machines to generate outputs on their own does not justify the logical leap to the concept of “machine authorship”: even Cohen admits that AARON’s autonomy “doesn’t extend to exercising judgment about what it’s doing.”²⁵⁷ Even the most sophisticated generative machines—those that employ adversarial neural networks to generate outputs²⁵⁸—are no more than complex sets of algorithmic instructions whose abilities are entirely attributable to how programmers train them with input data, and how programmers instruct them to analyze that input data. But these machines nevertheless pose difficult questions regarding the identification of a human author:

- Does Cohen “execute” the paintings that AARON generates? If so, does Cohen’s executorial stake in AARON’s creative process stem from his programming and training of the machine, or simply from his act of supplying the machine with paints and a power source and flipping the on/off switch? In the latter instance, does Cohen cede too much control over the execution of AARON’s paintings to forces outside of his control (like Chapman Kelley may have done with *Wildflower Works*)?

254. Cohen, *supra* note 250.

255. *Id.* (noting AARON’s capabilities as a “colorist”).

256. Bridy, *supra* note 3, at 15–18 (discussing Ray Kurzweil’s Cybernetic Poet and BRUTUS, an artificially intelligent “silicon author able to generate stories” created by Selmer Bringsjord and David Ferrucci in 2000); *see supra* note 210 (describing two music generation systems).

257. Cohen, *supra* note 250.

258. Generative adversarial neural networks models consist of two neural networks that work together to “bootstrap the learning process.” *Machine Creativity Beats Some Modern Art*, MIT TECH. REV., June 30, 2017, <https://www.technologyreview.com/s/608195/machine-creativity-beats-some-modern-art> [perma.cc/MRQ4-RQ6P]. Programmers might train the first network to recognize images of a specific type. For example, programmers might show the network thousands of paintings and label each painting according to its genre. Programmers might instruct the network to look for basic patterns in each painting, which might be indicative of its style category, and to adjust and refine its assumptions about the characteristics of a particular style by sorting through the set of training images. The second network would then generate random images and show them to the first network, which either “recognizes them as representing a particular artistic style or rejects them.” *Id.* Through trial-and-error and multiple repetitions, the second network “learns what the first network recognizes as art” and eventually “learns to produce images that match specific styles.” *Id.*

- If AARON produces a painting with color combinations and forms which surprise Cohen, can Cohen claim to have “conceived” of the paintings simply by training AARON to paint in a specific way? In other words, can Cohen claim that his creation of a generative machine with a range of potential outputs (some of which he might not actually imagine at the time of the machine’s creation) is just like the videogame programmer’s creation of a piece of software with a range of potential audiovisual outputs?

The analog world principles identified in Section II.D may provide some answers. As noted in that Section, copyright law does not always require an author to hold in her mind a precise mental image of the work she sets out to create. The essence of the conception requirement is the formulation of a complete *creative plan* for the work. A direct connection between the key aesthetic elements of the work—its contents, form, or compositional structure—and the author’s pre-fixation conception is not required as long as those expressive elements flowed directly from the author’s creative plan or conception.

Thus, the designers of fully-generative machines, such as AARON, which create works without further intervention or input from their users, can be the authors of the resulting outputs. These designers fully formulate a creative plan, manifested in the machines’ algorithms and processes, which will directly lead to the creation of expressive content. The lack of a direct connection between the designers’ minds and the expressive aesthetic content of the fully-generative machines’ output does not destroy the designers’ authorship claims any more than the lack of a direct connection between the nature photographers’ minds and the expressive aesthetic content of their works destroys those photographers’ ability to claim authorship over their images. The designer of the fully-generative machine thus meets the “conception” requirement of authorship. And as long as those designers, by designing the tool’s algorithms, or training a “learning” generative model to produce outputs, *control* the inner workings of the system, they have also *executed* the resulting works.

This conclusion remains true even if the designers of fully-generative machines have no chance to “adopt” the unanticipated expressive elements which result from the machines they build: for example, if their machines produce outputs after being sold to another user, or after the death of the

designer.²⁵⁹ Our examination of the photography examples shows that authorship status attaches to the wildlife photographer at the *moment of creation*—even if the photographer is not present when the camera fixes the image, she remains the author because of her executional stake in the work’s creation.²⁶⁰ Harold Cohen is the “author”—in the copyright sense, at least—of *all* the outputs of AARON at the time they emerge from the machine.²⁶¹

At first blush, it might seem strange that the designer of a fully-generative machine could be the author of the works that emerge from the machine, even if those works come into being after the end of the designer’s life. One might argue that the concept of posthumous authorship in copyright makes little sense because a creator who dies *before* a work comes into being has no opportunity to “sign off” on the finished work—to ratify the finished product as a suitable expression of the putative author’s mental conception. But we should not so hastily assume that the author’s post-fixation ratification is

259. Cohen, *supra* note 252 (jokingly expressing a desire to be the “first artist in history to have a posthumous exhibition of new work”). The concept of posthumous authorship may seem strange, but technological advancements have created similar situations before. For example, the development of artificial insemination has enabled men to conceive children after their death. See Brianna M. Star, *A Matter of Life And Death: Posthumous Conception*, 64 LA. L. REV. 613, 613–14 (2004) (noting the developments that have led to the problem of “posthumous conception,” how this development challenges “the validity of paternity and inheritance laws,” and the state-level legislative solutions, including the 2001 statute passed by the Louisiana state legislature allowing “most posthumously conceived children [to] attain legal status and inheritance rights”). Applied to copyright law, the possibility of a machine’s designer posthumous authorship results in abbreviated durations of the life-plus-70 copyright term. 17 U.S.C. § 302(a) (2018). Cohen died in 2016. See William Grimes, *Harold Cohen, a Pioneer of Computer-Generated Art, Dies at 87*, N.Y. TIMES, May 6, 2016, <https://www.nytimes.com/2016/05/07/arts/design/harold-cohen-a-pioneer-of-computer-generated-art-dies-at-87.html> [perma.cc/JDR9-FY8P]. If AARON creates a painting in 2066, and we assume that Cohen is the author of the work (because the machine is “fully-generative”), then the work will receive protection for only 20 years. If AARON produces a work in 2087, it will fall into the public domain *ab initio*.

260. See *supra* Section II.D (arguing that authorship in a photograph attaches at the moment of creation, whether or not the photographer-author is aware of the contents or has the opportunity to “adopt” the image after fixation).

261. Before Cohen died, his practice was to “start AARON running before [he went] to bed at night” and to “review” the “hundred and fifty originals . . . the following morning,” and “figure out which ones to print.” Cohen, *supra* note 252. Thus, Cohen discarded many of AARON’s creations, declining to “adopt” them as his own work. But while the disavowal of a work by a creator may mean that the work cannot be attributed to that creator as the artist, see 17 U.S.C. § 106A(a)(2) (2018) (granting the author of a “work of visual art” the right to “prevent the use of his or her name as the author” in certain circumstances), the disavowal does not mean that the creator is any less the “author”—in a copyright-law sense—of the work. See *infra* notes 262–267 and accompanying text (discussing the relevance of post-fixation ratification to authorship).

necessary to bring a work within the scope of copyright protection. Authors often decline to ratify the works they create: a photographer might capture hundreds of images and publish only one, discarding the rest as unworthy;²⁶² a painter might spend years generating sketches and figure studies before producing a final masterpiece. But even when authors explicitly disavow their disappointing works or early drafts, they remain the “authors” of those works or drafts (in a copyright-law sense) and retain the exclusive rights to prevent others from reproducing or displaying their works.²⁶³ The nature of a photographer’s decision not to publish most of her images does not mean that a third party who obtains her negatives (or memory cards) by rummaging through her garbage may freely exploit the disavowed works. Authorship attaches at the moment of creation and fixation—the author’s post-fixation approval or rejection of a work does not change the work’s status under the Copyright Act.

By contrast, ratification and post-fixation “sign off” may be relevant when an author employs the help of an amanuensis to execute her work. As we have noted, the relationship between artist and amanuensis is a principal-agent relationship: an artist-principal, like Alexander Calder, employs an amanuensis-agent, like the expert welders at Segre Iron Works, and specifies a specific task for the amanuensis-agent to complete.²⁶⁴ Within the scope of her delegated authority, the amanuensis may exercise *some* creative autonomy and may apply her expertise to the task at hand. When the artist reviews the completed work,

262. The photographer need not “adopt” the photographs post-fixation in order to be their author—the photographer’s authorship of her photographs attaches at the time of fixation. See *supra* Sections II.D & III.B.2.

263. Unfinished works are still covered by the Copyright Act as works of authorship—even if those works are abandoned. See *Mass. Museum of Contemporary Art Found., Inc. v. Buchel*, 593 F.3d 38, 47, 65 (1st Cir. 2010) (extending the Visual Artists Rights Act’s protection of an artist’s moral rights in original works of authorship to “unfinished creations that are ‘works of [visual] art’ within the meaning of the Copyright Act” even if the “artist becomes unhappy part-way through the project and abandons [the work]”); see also Daniel Grant, *Artistic Paternity: When and How Artists Can Disavow Their Work*, OBSERVER (July 28, 2016), <http://observer.com/2016/07/artistic-paternity-when-and-how-artists-can-disavow-their-work/> [perma.cc/MS4-ZD9D] (noting a dispute which arose when Frank Stella “placed some damaged artwork outside for trash pick-up only to find the work placed on exhibition at a Manhattan art gallery several months later,” and subsequently sued for the return of his work under 17 U.S.C. § 106A); *id.* (noting that Richard Prince “ripped up” 500 of his early works and “put them in garbage bags” but remained the “legal copyright holder for [the discarded works]” that were eventually found and sold to a number of galleries and museums, and thus retained the right to “refuse[] to allow any of their images to be reproduced in books or catalogues”).

264. See Knight, *supra* note 118 (“If he says it isn’t right, we do it over and over again until he’s pleased with it.”) (quoting Frank Pisani, the foreman at Segre Iron Works).

the artist's ratification or disapproval of the work may constitute a determination of whether the amanuensis-agent operated within the boundaries of the delegated authority. If the artist rejects the work of the amanuensis on the grounds that the amanuensis did not properly follow the artist's instruction, then that rejection may mean that the artist is neither the author in the art-world sense (i.e., the rejected draft work cannot be sold as the work of the artist) *nor* the author in the copyright-law sense. If the amanuensis produced the work outside the scope of her delegated authority, then the amanuensis—not the artist-principal—may be the author of the rejected draft work.²⁶⁵ But if the amanuensis hews to the author's commands, and the artist *still* rejects the work simply because the work did not turn out to be as aesthetically pleasing as the artist hoped, then the artist's rejection could *not* mean that she is no longer the author of the rejected or disavowed draft work. Instead, the artist's rejection of a work duly created by the obedient amanuensis is functionally the same as the artist's rejection of a work created by her own hand.

Author ratification, or post-fixation “sign off,” therefore is relevant only in situations in which the putative author needs to affirm that the work has been created under her executional control. The putative author's ability to reject the work of an amanuensis, or to demand revisions, may not alone suffice to establish that the putative author sufficiently controlled the work's execution,²⁶⁶ but when other indicia of control are present, author ratification can affirm that the task-assigner did in fact “mastermind” the work by verifying that the amanuensis did what the artist-principal wanted her to do.²⁶⁷ Applying these precepts to fully-generative machines, we understand that when an artist like Harold Cohen builds a machine such as AARON, capable of producing new works without any creative input from the person who operates the

265. In these situations, the work produced by the amanuensis may be a derivative work based on the instructions of the principal artist, if the principal artist's instructions meet the qualifications for a standalone work of authorship. If so, and if the rejected derivative work were considered infringing (the artist having revoked her permission to create it), then the principal artist could prevent the amanuensis' exploitation of the unauthorized derivative work. *See* 17 U.S.C. § 103(a) (2018) (“[P]rotection for a work employing preexisting material in which copyright subsists does not extend to any part of the work in which such material has been used unlawfully.”).

266. *See* *Geshwind v. Garrick*, 734 F. Supp. 644 (S.D.N.Y. 1990) (holding that a task assigner who asked an artist to create a 15-second animated sequence was not the author of the resulting work, even though the task assigner had retained the right to approve the artist's work and to demand revisions).

267. *See* *Lindsay v. Wrecked & Abandoned Vessel R.M.S. Titanic*, 1999 WL 816163, at *5 (S.D.N.Y. Oct. 13, 1999) (noting that the director had “screened the footage at the end of each day to ‘confirm that he had obtained the images he wanted’”).

machine (other than turning it on), there exists no doubt that the machine is faithfully carrying out the executional commands of the machine's designer; as Cohen's agent, AARON is incapable of going off "on a frolic of his own." Moreover, AARON's outputs are all incipient from the moment Cohen programmed and trained the machine, and no third-party intervention will alter them. Thus, the inability of the designer to ratify or "sign off" on the works produced by the machine is not a valid reason to deny that designer's authorship of the resulting work—even if the work is produced after the author's death. In these circumstances, the designer remains the output's "author," whether he is across the room, across town, or across the River Styx.

3. *Partially-Generative Machines: Those Whose Outputs Reflect a Combination of the Creative Contributions of Designer and User*

The final (and most problematic) category of generative machines are "partially-generative"—machines whose outputs reflect the creative contributions of both the designer and the user. These machines do not wholly generate the expressive content of the resulting works, but instead rely on the creative contributions of users. French artist and computer scientist Patrick Tresset developed a drawing machine he calls "Paul" which takes a photograph of a human subject, processes the image, and uses a robotic arm to generate a portrait sketch of the subject.²⁶⁸ Tresset cannot anticipate Paul's outputs—they depend on the image captured by its camera—but all of Paul's sketches share expressive elements with Tresset's own artistic style: messy lines, dark shading, and sharp contrasts:

268. P. A. Tresset & F. Fol Leymarie, *Sketches by Paul the Robot*, COMPUTATIONAL AESTHETICS IN GRAPHICS, VISUALIZATION, AND IMAGING (2012), <http://doc.gold.ac.uk/~ma701pt/patricktresset/wp-content/uploads/2015/03/p17-tresset.pdf> [perma.cc/54B2-SKUE].

Figure 6: Paul's sketches²⁶⁹

Tresset programmed Paul's drawings to emulate his own; they share a common aesthetic, technique, and style attributable directly to Tresset. But, importantly, while the programmer has determined the drawings' form, he has not selected their subjects:²⁷⁰ the person who operates the machine decides who the drawings will depict, and to some extent how the subject will appear (facial expression; framing of the image). This operator, of course, may in many instances be Tresset himself. But the operator could easily *not* be Tresset. Suppose Tresset sells Paul and its purchaser uses the drawing machine to create portraits of her closest friends. The purchaser asks her friends to pose in front of Paul and wait while the machine generates drawings of each of them. Neither human participant—Tresset nor the operator—is *solely* responsible for the expressive content in the resulting drawings. Both participants have

269. *Id.*

270. Admittedly, neither do the wildlife photographers in the hypotheticals above—and neither does Harold Cohen, who may train AARON with basic forms, but does not tell AARON what to paint. But here, some other creator fills the “gap” between what Tresset determines and the resulting work (by supplying the subject of the drawings). We are content to conclude that wildlife photographers author their works even without entirely determining their contents because the natural or random forces fill the “gap” between what those photographers determine (i.e., the lens, the focus, the framing, etc.) and what the photographs depict. And we are content to conclude that Cohen is the author of AARON's outputs because the randomness Cohen programmed into his machine makes uncertainty as to what AARON will depict a part of the process. But when another human being, whose creative decisions are relevant to the work's final form, fills that “gap,” we must more carefully question whether the first creator (here, Tresset) can claim to be the sole author of the resulting work.

contributed creatively to the result—Tresset contributed his general artistic style, and the user contributed the application of this style to a particular subject. The contributions of both participants have merged, inseparably, in the resulting drawings.²⁷¹

Consider a different example of a partially-generative tool: Google’s AI Duet, which lets users “play a duet with [a] computer.”²⁷² Google’s engineers invite users to “play some notes” on a digital keyboard, and implement a machine learning algorithm trained to “respond to [the user’s] melody.”²⁷³ AI Duet generates a somewhat unpredictable accompaniment to the user’s melody, and simulates the effect of an improvisational piano duet (although not very well).²⁷⁴ The user’s melody is her own creation, but who is the author of the accompaniment? Like Paul’s drawings, the final melody is a product of both the engineers who “trained” A.I. Duet’s learning algorithm,²⁷⁵ and the user who inputs the melody to which A.I. Duet responds. The contributions of both participants have thus merged inseparably—the designers supply the machine with basic musical knowledge, which the user then summons into action by supplying a melodic line.

Partially-generative machines create several difficult authorship questions:

- Who—the user of the machine, or the designer of the machine—is the person responsible for the creative plan that determined the work’s expressive content? We have noted that the designers of fully-

271. In this hypothetical, Tresset and the user would not be able to claim co-authorship of a “joint work” for lack of mutual collaborative intent (i.e., Tresset is not aware of the user’s contribution to the final work, and thus cannot have the intent to merge his contributions with those of the user). *See supra* Section II.F (discussing co-authorship doctrine).

272. Yotam Mann, *AI Duet: A Piano That Responds to You*, GOOGLE: AI EXPERIMENTS (May 2017), <https://experiments.withgoogle.com/ai/ai-duet> [perma.cc/A863-VS2B].

273. *Id.* (noting that AI Duet is powered by machine learning).

274. Comparing AI Duet with a real piano duet bolsters the argument that artificial intelligence is, at least in its current form, far from reproducing human ingenuity. *Compare* Payette Forward, *Google AI Duet with Keyboard*, YOUTUBE (Feb. 17, 2017), <https://www.youtube.com/watch?v=QiMWnOPMzb0> [perma.cc/3BMC-55MM] *with* Herbie Hancock & Chick Corea, *Recording of Concert in Frankfurt, Germany*, YOUTUBE (Feb. 18, 1978), <https://www.youtube.com/watch?v=2zir6HqjDMo&t=1413s> [perma.cc/C273-5MHU].

275. *See* Google Developers, *A.I. Experiments: A.I. Duet*, YOUTUBE (Nov. 15, 2016), <https://www.youtube.com/watch?v=0ZE1bfPtvZo> [perma.cc/V2Q7-4BZK] (“If I was trying to make A.I. Duet with more traditional programming, I’d have to write out lots of rules. Like if someone plays a C, then maybe respond [sic] by going up to a G. . . . I’d basically be creating this map to tell the computer how to make these decisions. . . . This experiment approaches the problem differently, using machine learning, specifically neural networks. We played the computer tons of examples of melodies. Over time, it learns these fuzzy relationships between notes and timings, and builds its own map based on the examples it’s given.”).

generative machines may be the authors of the resulting works even if they do not have any pre-fixation mental image of what the machines will create (see discussion of AARON and fully-generative machines, above). But we have also noted that, with respect to partially-generative machines, both designer and user contribute creatively to the final work. Does the user's provision of a creative contribution interrupt the designer's authorship claim to everything her machine creates?

- Does the user of the partially-generative machine “control” it in such a way that allows that user to claim to have executed the resulting work? On the one hand, the programmers of these machines are primarily responsible for *how* the machine works and thus might be the parties who “guide and inspire” the means of creation. But on the other hand, the users of these machines may, in some circumstances, exercise control over the machine by supplying the requisite inputs or by harnessing the machine's processes in order to create a particular result—and thus might control the process of creation in the same way that a user controls a sophisticated digital camera.
- If the person responsible for the conception of the work (who might be the user) is not the person responsible for the execution of the work (who might be the designer), can either of them claim to be the author of the result? Are they co-authors? Or is the work “authorless”?

As a preliminary matter, copyright's rules regarding co-authorship may restrict the ability of the designer and the user to claim that the resulting work is a “joint work” if the two participants neither know each other nor collaborate contemporaneously. This Article reexamines the requirements of co-authorship in Section IV.B. But assuming no co-authorship, the crucial inquiry is how to allocate the essential elements of authorship (conception and execution) to the participants involved. As discussed, only a creator who participates in both processes—contributing mentally to the conception of the work, and contributing physically to the execution of the work—can claim sole authorship.

The above questions reduce to two essential inquiries: First, at what point does a user's input become significant enough to justify departing from the rule that the designer of the machine (like the wildlife photographer) is necessarily the author of the result? In other words, what is the distinction between a fully-generative machine and a partially-generative machine? Second, at what point does the user exert control over a generative machine? The following Section examines these questions.

C. AUTHORSHIP AND PARTIALLY-GENERATIVE MACHINES

1. *Distinguishing Between Fully- and Partially-Generative Machines: Can the Upstream Creator Claim Ownership of All Resulting Outputs?*

a) Describing the Distinction

The fundamental difference between fully- and partially-generative machines must be the scope of possible creative decisions supplied by the machine's user. As we have shown, the outputs of fully-generative machines—those which can create works on their own, with minimal user input—are the works of the machine's designer. Because the designer of the machine sets up a process which will lead to the creation of the work without the contribution of any other creative forces, the designer will be the author of the end result, even if that author has little specific conception of what will come out of the machine.²⁷⁶ And the *user* of such a machine, who simply turns the machine on, has no authorship stake in the result, and merely fulfills a limited step in the designer's creative plan. Consider, again, *Naruto Version Three*: Slater sets up his camera in the Sulawesi jungle, sets it on an autotimer which will snap the shutter at predetermined time intervals, and then leaves the scene. If Slater instead hired an apprentice and, after setting up the camera, instructed the apprentice to wait beside the camera and snap the shutter at the same predetermined time intervals, Slater would not forfeit his authorship claim, and the apprentice would not become the author.²⁷⁷ Similarly, the designer of a machine—who sets up the entire process of creation—does not lose her authorship claim simply because she allows someone else (a user) to press the initiating button.

This logic still applies even if the user has some limited choices while operating the machine. Consider, for example, some basic music generation algorithms. JukeDeck is a software system that “brings artificial intelligence to music composition and production” and uses “deep neural networks to understand music composition at a granular level.”²⁷⁸ JukeDeck prompts users to input basic parameters like tempo, genre, instrumentation, duration, and climax, and then produces a musical work based on the defined parameters.²⁷⁹ JukeDeck's users need not supply a melody, a key signature, or a chord structure—JukeDeck's neural network generates these aspects of the

276. *See supra* Section III.B.2 (discussing fully-generative machines).

277. The apprentice could be compared to Sarony's cameraman, who operated the camera but did not become the author of the resulting picture. *See Farley, supra* note 2, at 434.

278. *About*, JUKEDECK, <https://www.jukedeck.com/about> [perma.cc/H8C5-MX8Z] (last visited Apr. 6, 2018).

279. *Id.*

compositions itself. Its users supply nothing that even approaches a protectable “expression”—defining the tempo or genre of a musical composition may influence the type of composition generated, but it does not determine the expressive content of the output.

We might think of JukeDeck as another fully-generative machine, like Harold Cohen’s AARON. That the user can choose from a range of parameters should not make a difference. Consider a simplified version of JukeDeck, which allows users to choose only the genre of the resulting piece (i.e., classical, rock, or jazz). The user’s genre selection does not mean that the user exercises any influence over the conception or the execution of the result. This simplified version of JukeDeck is essentially three music generation algorithms jammed into a single box: by choosing one of three genres, the user is choosing which of three machines (i.e., the classical music generator, the rock generator, or the jazz generator) to activate. That this user springs the machine into action by choosing which genre-machine to activate should not disturb the conclusion that the machine’s designer is the sole author of the result. And introducing additional options (i.e., allowing the user to choose tempo, genre, instrumentation, etc.) should similarly not change the analysis.

This logic, however, must have a limit. At some point, the user’s choices when operating the machine will interrupt the designer’s claim of authorship of the machine’s outputs. Consider a modified version of *Naruto Version Three*: Slater sets up a camera in a public wildlife reserve by pointing it at a grove of trees where macaque monkeys often congregate, and offers visitors the opportunity to approach the camera, wait for macaques to wander through the scene, and snap a photograph at the moment of their choosing. While Slater has certainly supplied *some* creative influence over the resulting photographs (by framing the image and selecting the type of lens, etc.), the originality inherent in the resulting images is mostly attributable to the visitors who snap the photographs.²⁸⁰ A visitor who waits by the camera and then snaps the shutter at what she perceived to be the perfect moment, capturing an image of a troop of macaques congregating in the grove, has a strong claim

280. In this situation, Slater might argue that he is at least a co-author due to his creative contributions to the result (framing the image and selecting the type of lens). But simply supplying the equipment does not make one a co-author, and Slater may not be able to claim that the resulting photograph is a “joint work” unless he collaborated with the visitor who ultimately pushed the button. *See* *Nottage v. Jackson* [1883] 11 QBD 627; *infra* Part IV (discussing co-authorship doctrine).

of authorship in the image because that user supplied an essential element of originality in a photograph: originality in timing.²⁸¹

Similarly, if a user of a generative machine exercises some creative influence over the expressive contents of the resulting work, then it would be inappropriate to assume that the designer of the machine is the sole author of the result. The user's creative contribution interrupts the designer's authorship claim. One might frame this conclusion in terms of *conception*: because the designer of the machine has built it to require the creative contribution of an end-user, the designer of the machine cannot claim to have conceived of each of the potential results. In other words, the designer's creative plan (or conception) is *incomplete* without the creative contributions of the user. Herein lies a crucial (and difficult) question: at what point does the user of a generative machine exercise sufficient influence over the result to interrupt the authorship claim of the machine's designer? At what point does the machine's designer rely *too much* on the contribution of the end-user, such that the designer's creative plan for the work is incomplete? And, finally, does the user's interruption make her the (or "an") "author" of the output?

b) Prior Judicial Approaches to This Question

Some courts have considered similar questions in deciding cases involving generative machines. In *Torah Soft Ltd. v. Drosnin*,²⁸² the plaintiff designed a computer program for "Bible code research"—the enterprise of "foretell[ing] future events" by examining a "code . . . revealed by finding words and phrases

281. *Mannion v. Coors Brewing Co.*, 377 F. Supp. 2d 444, 453 (S.D.N.Y. 2005) (describing originality in timing). Note, however, that this logic might break down if Slater pointed his camera at a subject that did not vary with the passage of time. For example, consider a museum curator who installs a Polaroid camera directly in front of a sculpture, fixes the camera in place and adjusts the room's lighting to create a perfect image of the artwork, and invites visitors to press the camera's shutter button to produce an image of the statue to take home as a memento. Each visitor who presses the camera's shutter button will produce an identical image. Like Sarony's apprentice, who may have chosen the precise timing of the famous Oscar Wilde photograph but who did not "compose" the image, the visitors would not become authors simply by pressing the camera's button. Because the camera is fixed in place, the visitors may influence only the *timing* of the photograph, which will not influence the content of the resulting image. And like Sarony himself, who "produced the [Oscar Wilde] photograph" by "posing the said Oscar Wilde in front of the camera," the person who set up the museum's camera would be the author of the photograph because she is entirely responsible for the content of the resulting images. See *Burrow-Giles Lithographic Co. v. Sarony*, 111 U.S. 53, 60 (1884). Therefore, the authorship question might depend on the elements of originality reflected in the result, and to whom those elements are attributable.

282. *Torah Soft Ltd. v. Drosnin*, 136 F. Supp. 2d 276 (S.D.N.Y. 2001).

which appear in the [Hebrew] Bible at equidistant letter skips.”²⁸³ The software, “in response to an end-user’s input of a particular term, sift[ed] through [a] Database [of Biblical texts], reorganize[d] it according to its algorithm, and then create[d] a matrix” of Bible code in which the search term appeared.²⁸⁴ The software’s results were “repeatable whenever the input is identical. . . . That is to say, each time an end-user inputs the phrase ‘Yitzhak Rabin,’ the Software [would] produce the same matrix.”²⁸⁵ The court sought to determine, *inter alia*, whether the user of the software, who “merely inputs a word or phrase which the Software searches for in the Database,”²⁸⁶ could claim ownership over the software’s output. The court held that the user of the Bible code software could not claim ownership of the outputs.²⁸⁷ The court noted:

Although the matrixes [produced when a particular user inputs a particular search term] do not appear either in the Software or the Database, they are ‘fixed’ insofar as the output is repeatable whenever the input is identical. . . . [A]n end-user’s role in creating a matrix is marginal. . . . Creating a matrix is unlike the creative process used in many computer art programs, which permit an end-user to create an original work of art in an electronic medium. . . . [U]sers of such programs often supply the lion’s share of the creativity to create the screen display. . . . By contrast, an end-user of the Software merely inputs a word or phrase which the Software searches for in the Database. Thus, the Software does the lion’s share of the work.²⁸⁸

In *Rearden, LLC v. Walt Disney*,²⁸⁹ by contrast, the plaintiff (Rearden) owned the “MOVA Contour Program,” a program used in filmmaking that “precisely captures and tracks the 3D shape and motion of a human face,” thus “captur[ing] an actor’s performance frame-by-frame” and creating output files which filmmakers can use “for many different applications, such as ‘retargeting’ the actor’s face onto another real or fictional face.”²⁹⁰ Rearden claimed that the defendants used its program to create several films, including *Beauty and the Beast*, *Deadpool*, and a *Terminator* franchise film, and that it did not

283. *Id.* at 280.

284. *Id.* at 283.

285. *Id.*

286. *Id.*

287. *Id.* at 283. The court eventually held that the outputs were not sufficiently original to merit protection. *See id.* at 292 (granting the defendant’s motion for summary judgment after noting that the “[p]laintiff has failed to satisfy its burden of proving that the Software’s outputs of Bible code finds, as displayed in the matrixes, contain protectable expression”).

288. *Id.* at 283.

289. *Rearden, LLC v. Walt Disney*, 293 F. Supp. 3d 963 (N.D. Cal. 2018).

290. *Id.* at 967.

authorize the studios to use its programs. Rearden claimed that because “the MOVA Contour program performs substantially all the operations in creating the [film] output,” Rearden, as the owner of the program, is the “author of the output”—that is, of the footage produced using the technology.²⁹¹

The District Court for the Northern District of California focused on the language from *Torab Soft*,²⁹² noting that “Rearden must adequately plead that the MOVA Contour program does the ‘lion’s share’ of the creating and that the end-user’s role in creating the final product is marginal” in order to prove ownership of the output.²⁹³ The court ultimately found that the studios, not the creator of the program, authored the outputs:

The court does not find it plausible that the MOVA Contour output is created by the program without any substantial contribution from the actors or directors. Unquestionably, the MOVA program does a significant amount of work But this cannot be enough, since all computer programs take inputs and turn them into outputs. . . . Here, Rearden must allege that the MOVA program has done . . . “the lion’s share of the creativity” in creating the outputs. . . . Here, unlike in *Torab Soft*, where the user merely inputs a word into the program, MOVA Contour’s user inputs a two dimensional camera capture that may range from [an actor’s] facial expressions . . . to the [actor’s] subtle and dynamic motions.²⁹⁴

The courts in *Torab Soft* and *Rearden* seemed to analyze two issues simultaneously: first, whether the outputs of the programs in question “reflect[] the program’s contents,” and second, whether the program or the user does the “lion’s share of the work” to create the output.²⁹⁵ But the courts’ analyses trained on the question identified above: whether the user’s contribution was necessarily limited (as it was in *Torab Soft*), or whether the user’s contribution constituted the “lion’s share of the creativity”²⁹⁶ and thus superseded the authorship claim of the designer of the program (as was the case in *Rearden*).

But the *Torab Soft/Rearden* test deals primarily with the distinction between (i) ordinary tools—whose outputs reflect only the creative contributions of the

291. *Id.* at 969.

292. The court also referred to a Ninth Circuit case on a similar issue, which drew its reasoning from *Torab Soft*. See *Design Data Corp. v. Unigate Enter. Inc.*, 847 F.3d 1169 (9th Cir. 2017).

293. *Rearden*, 293 F. Supp. 3d at 970–71.

294. *Id.* at 971.

295. *Id.* at 970 (quoting *Design Data*, 847 F.3d at 1173).

296. *Id.*

user (as was the case in *Rearden*), and (ii) fully-generative machines—whose outputs reflect only the creative contributions of the machine’s designer (as would have been the case in *Torah Soft*).²⁹⁷ In these cases, it seems simple to allocate authorship to either the machine designer or the user: the outputs will entirely reflect the creative plan of either the machine’s designer (*Torah Soft*) or the user (*Rearden*). The *Torah Soft/Rearden* test does not, therefore, provide much guidance to determine the distinction between (i) fully-generative machines—whose outputs reflect only the creative contributions of the machine’s designer, and (ii) partially-generative machines—whose outputs reflect a *combination* of the creative contributions of designer and user.

For example, the *Torah Soft/Rearden* test does not help determine the proper author of Paul’s portrait sketches.²⁹⁸ As noted, these drawings reflect the contributions of both designer and user: Tresset (Paul’s creator) has programmed the machine to draw, and the user contributes the human subject, determining not only the identity of the human subject, but the expression on the subject’s face and how the subject’s face is framed within the sketch. To the extent that Tresset’s style appears in the resulting drawings, this style does “reflect the program’s contents,” and Tresset’s machine does “the lion’s share of the work” to apply this style to whatever image the user supplies to the machine. But the resulting work, as a whole, does not “reflect the program’s contents” because the particular faces depicted in the sketches are not inherent within the machine itself.

c) Approaches to the Distinction Between Fully and Partially Generative Machines

How, then, should we approach the question of whether the user’s participation in the creative process interrupts the authorship claim of the machine’s designer? One potential distinction is whether the user supplies anything *new* to the machine, or whether the output is necessarily a rearrangement of elements already within the machine. One might argue that, if the output of a generative machine is composed solely of elements inherent within the machine, then the machine is fully-generative (and thus its designer is the author of the outputs). This approach mirrors the approach in the videogame cases discussed in Section II.E, in which the courts suggested that

297. As noted above, the *Torah Soft* court found that the Bible code matrices were not sufficiently original to merit copyright protection. *See Torah Soft v. Drosnin*, 136 F. Supp. 2d 276, 292 (S.D.N.Y. 2001).

298. *See supra* note 268 and accompanying text (discussing “Paul,” a drawing machine created by Patrick Tresset).

the videogame player does not interrupt the designer's authorship claim by simply rearranging elements stored within the game and composed by a game's designer.

But even within the context of videogames, this logic only goes so far. Minecraft, for example, a game which invites the player to "make things out of virtual blocks, from dizzying towers to entire cities"²⁹⁹ supplies its players with basic building blocks which they can use to create an infinite array of structures, cities, or vessels. "Nearly everyone who plays Minecraft, or even watches someone else do so, remarks on its feeling of freedom: All those blocks, infinities of them! Build anything you want! Players have re-created the Taj Mahal, the U.S.S. Enterprise from 'Star Trek,' the entire capital city from 'Game of Thrones.'"³⁰⁰ Few would argue that a player who spends years using Minecraft to imagine and construct her dream mansion (complete with guest house, pool, bowling alley, and four-car garage) would not be the "author" of the resulting model, or that the programmer of Minecraft would have any authorial stake in the resulting work. However, each of these results is "implicit" in the game itself—the players of the game do not introduce any unanticipated elements into the game, but simply rearrange the pre-existing blocks to generate their own creations. It seems odd to extend the logic of the videogame cases to situations in which the players recombine elements of a game in a way that reflects a substantial amount of player creativity.³⁰¹

One could even argue that the user of Microsoft Word simply recombines and rearranges elements (letters, fonts, formatting styles, etc.) which already exist within the program. Of course, few (if any) would argue that the logic of the videogame cases could apply to Microsoft Word—a person who types and formats a Word document is the author (or one of the authors) of the resulting document.

Asking whether the downstream user of a machine contributes something *new* to the machine's creative process therefore cannot be the operative question. That approach fails because a user can exercise sufficient creativity by combining and recombining elements that already exist in the machine.

299. Clive Thompson, *The Minecraft Generation*, N.Y. TIMES MAG., Apr. 14, 2016, <https://www.nytimes.com/2016/04/17/magazine/the-minecraft-generation.html> [perma.cc/7A3Y-Y7PB] ("Blocks can be attached to one another to quickly produce structures. Players can also combine blocks to 'craft' new items.").

300. *Id.*; see also Boyden, *supra* note 207, at 387 (noting that modern videogames may be distinguishable from the videogames that formed the basis of the videogame cases from the 1980s because modern games allow users slightly more creative autonomy).

301. See *supra* note 125 (discussing whether the logic of *Stern* and the other videogame cases should apply to modern videogames).

There is no categorical difference between users who supply new *content* to a machine (i.e., Paul's users supply the drawing machine with a new human subject to draw) and users who supply new and unanticipated *arrangements* of elements that already exist within a program.

This Article proposes a more effective test: when the upstream creator's decisions define and bound the downstream creator's role, the downstream creator does not disrupt the upstream creator's claim of authorship.³⁰² In these circumstances, the upstream creator has effected a limited delegation of creative control to the downstream creator, who simply completes the upstream creator's creative plan by making a relatively foreseeable choice—pushing a button, choosing between a limited set of parameters or settings, or moving a joystick to proceed through a simple videogame. But when the upstream creator's creative plan for the work does not limit the downstream user's creative autonomy, and instead relies on the downstream creator to endow the work with additional (and unforeseeable) creative content, the upstream creator cannot claim to be the sole author of the resulting work because she has not crafted a complete creative plan for the work's production.

To determine whether the upstream creator has sufficiently “bounded” the downstream creator's role, one might ask whether the upstream creator *could have anticipated* what the downstream user would do to “complete” the work.³⁰³ If it was possible for the designer of the machine to anticipate *every* potential

302. For example, the programmers of the videogames addressed in *Stern Elecs, Inc. v. Kaufman*, 669 F.2d 852 (2d Cir. 1982), and its progeny sufficiently bound the roles of their downstream users, whose movement of the game console's joysticks and whose navigation through the relatively simple games was foreseeable and anticipated by the programmers and thus part of their “creative plans.”

303. This approach may create some tension with the wildlife photographer hypotheticals addressed above. In Section II.D.2, this Article noted that such a photographer need not have *any* aesthetic pre-execution conception of what her camera would capture. One might argue that Zapruder could not have anticipated that his attempt to film “home videos” of the presidential parade would end up capturing the assassination of President Kennedy—yet he remained the author of the footage. To use a more extreme example, if in *Naruto Version Three* Slater's auto-timed camera ended up snapping a photograph of an alien invasion of Sulawesi, one might *still* recognize that Slater is the author of the resulting footage even though he could not have anticipated the result. In situations involving only a single creator (the sole creative contributor), one can assume that the creator (like the nature photographer) is the author even if she did not anticipate the resulting work, because she has fully formulated the creative plan for the work (and any unanticipated variation is attributable to nature, or in the case of Cohen's AARON, some combination of randomness and the complexity of the machine). But when another potential author (the downstream user) has supplied some creative input, we must investigate whether that author's contribution has disrupted the first author's claim, i.e., whether the first author's creative plan for the work was incomplete.

resulting work, the designer can claim that her creative plan encompassed each of the resulting works. But if the designer of the machine, at the time of her participation in the creative process, could *not* have anticipated how the user of the machine would complete the work, then the designer cannot claim sole authorship³⁰⁴ of any of the resulting works because these resulting works were not entirely the product of the designer’s creative plan, which must have been incomplete without the creative contribution supplied by the user.³⁰⁵ This test would *not* inquire whether the machine’s designer *actually* anticipated the result³⁰⁶—such an approach would be impossible to administer (because the designer could always *claim* to have anticipated a particular result).³⁰⁷

The proposed *possible anticipation* test is consistent with the result of the early videogames cases: with simple videogames like Space Invader or Pacman (which the courts in the videogame cases considered), it would have been entirely possible for the games’ designers to have anticipated any of the resulting audiovisual sequences. The test would also encompass more complex games, such as Tetris or Candy Crush, because the programmers *could have* anticipated any given output of the game when they designed the game (even if the programmers did not in fact anticipate a particular output). But this test would deny authorship to the programmers of Minecraft, who, due to the vastly increased possibilities for player intervention within the game, would be

304. For a discussion of whether the designer can claim co-authorship with the machine’s user, see *infra* Part IV.

305. Note that this approach is consistent with the “master mind” concept of authorship introduced in Part II. In other words, the designer of the fully-generative machine is the “master mind” of the resulting work even though she left the final generation of the work to a user empowered to choose between a foreseeable range of potential inputs or instructions (i.e., input that could be *anticipated* by the designer). But the designer of the machine is *not* the “master mind” of the work if she designed a machine that would necessarily produce results that the designer could not have anticipated, because the range of potential user inputs is similarly impossible to anticipate.

306. This actual anticipation approach is similar to another potential approach: whether the machine has a finite number of potential outputs. If the machine’s outputs are infinite in scope, then it would be impossible for the designer of the machine to have *actually anticipated* each potential output. But this quantitative approach does not help to explain the videogame cases, assuming that the range of potential arrangements of pre-existing audiovisual components in a videogame is infinite.

307. Admittedly, the proposed *possible anticipation* approach may pose its own administrability problems. The purpose of this Article is not to propose a bright-line rule, but instead to elucidate a principle—consistent with the “analog” authorship principles of “conception” and “execution” outlined in Part II—sufficient to clarify the necessary distinction between fully-generative machines (whose outputs are presumptively works of authorship attributable to the machine’s designer) and partially-generative machines (whose outputs may be works of sole authorship attributable to the machine’s user, works of joint authorship, or “authorless”).

unable at the time of their participation in the creative process (when they designed the game) to anticipate what the game's players would build. Like the programmers of Microsoft Word, who cannot anticipate all the works that users will create using the word processing program, the designers of Minecraft provide a set of pre-defined elements, but players can combine those elements in ways the programmers neither expect nor determine. This approach would similarly deny authorship to Tresset—the creator of Paul, the drawing machine. Because Tresset cannot anticipate which faces Paul will sketch, Tresset cannot claim to be the author of the resulting drawing (assuming, of course, that someone other than Tresset operates Paul and chooses the subject to depict).

2. *Dealing with Partially-Generative Machines: Who Executes the Work?*

The conclusion that a machine is partially-generative (and thus that the designer of the machine cannot claim sole authorship of the resulting works) does not necessarily mean that the *user* of the machine is the author of the resulting work. One might safely conclude that the user of such a machine *conceived of* the resulting work, because the user provides some unanticipated contribution to the machine to create the result (otherwise, the machine would be fully-generative and authorship of the result would go to the machine's designer). But conception supplies only half of the authorship equation. The user of such a machine can claim authorship of the result only if that user sufficiently controlled the process through which the work came into being. If the user does control this process, then the user has both conceived of and executed the resulting work, and is therefore the sole author of the resulting work just like the user of an "ordinary tool." Moreover, as discussed previously in this Article, a contributor who supplies only conception cannot "adopt" the resulting work if that creator plays no part in the execution of the work.³⁰⁸

There may be some tension between the assertion that a photographer "controls" her camera (and thus executes the work that the camera produces) and the assertion that the user of a generative machine (that she did not create), who provides the conception for the resulting work, does not "control" the machine and thus does not "execute" the resulting work. In other words, the photographer is capable of "controlling" her camera by simply manipulating the camera's user interface (its buttons and dials) and pointing the camera in a specific direction—the complexity of the process that occurs inside the camera, and the photographer's comprehension of that complexity, are not relevant to whether the photographer *executes* the work that the camera

308. See *supra* Section II.D.1.

physically produces. So why should the user of a more sophisticated generative machine, like a generative machine-learning model, not also “control” that model when she turns it on and supplies it with instructions?

The key to this distinction is that the photographer, by operating the camera, *inevitably controls how* the camera operates, and thus *executes* the work. A camera, in other words, is not *self-operating*—the user must instigate every movement and function the camera accomplishes. The photographer might point a camera in a particular direction, choose a particular time of day during which to take a photograph, focus the camera or use an autofocus function, and select the right moment at which to click the shutter (or implement a timed shutter feature). To be sure, these are *expressive* acts, but they are also acts of *execution*—acts which necessarily define how the work will come into physical being.³⁰⁹ And even though some photographers are considerably less involved in this process (think, for example, of a photographer who uses only point-and-click disposable cameras), these photographers are still closely involved with the process of execution: they define *what* the camera captures, and *when*. The physical involvement of the human being in operating the camera will always determine *how* the camera captures an image. Even if two people, with two identical cameras, have identical *conceptions* of what they wish to capture, their individual operation of their cameras will always result in two distinct images—two separate and individual executional processes.³¹⁰ As Judge Learned Hand observed in 1921, “no photograph, however simple, can be unaffected by the personal influence of the author, and no two will be absolutely alike.”³¹¹

Users of generative machines, however, might not have to fulfill any of these executional functions in order to generate an output. Suppose the Little Prince buys a general-purpose drawing machine and commands it to “Draw me a sheep.” He will have furnished a general idea that the machine will convert into a drawing without any further participation from the imperious

309. Without these acts of execution, the user of the machine cannot claim that the machine is her “agent” because she has not influenced *how* the machine carries out its tasks. *See supra* notes 59–70 (characterizing the author-amanuensis or author-tool relationship as one of agency, and noting that the author-principal must influence the agent’s execution in order to claim ownership over the result).

310. *Cf.* Ron Risman, *How Two Photographers Unknowingly Shot the Same Millisecond in Time*, PETAPIXEL (Mar. 7, 2018), <https://petapixel.com/2018/03/07/two-photographers-unknowingly-shot-millisecond-time/> [perma.cc/6FW8-9YYP] (noting how two photographers inadvertently captured strikingly similar images of a wave crashing against a lighthouse in New Hampshire). *But see id.* (noting that the images were “slightly different”).

311. *Jewelers’ Circular Pub. Co. v. Keystone Pub. Co.*, 274 F. 932, 934 (1921).

little boy. The Little Prince's instruction might influence *what* the machine seeks to portray, but the instruction does not influence *how* the machine converts that general idea into a final work.³¹² Two users who provide identical instructions to the general-purpose drawing machine will necessarily receive the same result—unless, of course, the machine is programmed to vary its outputs randomly. But in such a case, the variation in the output would be attributable not to differences in what the users did, but to a decision by the machine's designer.

Consider, for example, someone who uses Google Translate to translate this Article from English into French. The user inserts the text of the Article into the Google Translate website, which in its latest form,³¹³ uses a sophisticated machine-learning model to translate the text into French. By simply supplying the text, the user exercises no influence over *how* Google's algorithm translates it into French.³¹⁴ The programmers of the Google Translate algorithm, who are responsible for training the neural network to understand both the English and French languages, entirely control the process through which the resulting work (the translated article) comes into being. Two users who input the same text into Google Translate will get the same result, and neither user can tweak Google's algorithm to create a different output given the same input. Google Translate does not provide any user-defined parameters for users to change *how* the translation algorithm works; users cannot ask the algorithm to favor certain phrasings or resolve

312. We might compare this situation to the creation of the "Next Rembrandt" by a team of art historians and computer scientists using a generative machine. The process of creating the "Next Rembrandt" involved a single team of scientists and art historians who influenced both the *what* and the *how*—and thus these scientists should be considered, collectively, the authors of the resulting painting. *See supra* note 213 (describing the "Next Rembrandt" project).

313. Recently, Google has used a neural network to improve its Google Translate service. Rather than "program[ming] into the computer all of the grammatical rules of [each language], and then the entirety of definitions contained in the [lexicon]," the use of neural networks attempts to "produce multidimensional maps of the distances, based on common usage, between one word and every single other word in the language"—"[t]he machine is not 'analyzing' the data the way that we might, with linguistic rules that identify some of them as nouns and others as verbs. Instead, it is shifting and twisting and warping the words around in the map. . . . Some of the [developments in Google's translation system were] not done in full consciousness. [The researchers] didn't know themselves why they worked." Gideon Lewis-Kraus, *The Great A.I. Awakening*, N.Y. TIMES MAG., Dec. 14, 2016, <https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html> [perma.cc/4LCL-5CTK].

314. *See supra* discussion of *Nottage v. Jackson* [1883] 11 QBD 627 (Eng.) (holding that a party who instructed a hired photographer to take the picture of an Australian cricketer did not become the author of the resulting photograph because the photographer was the "originator in the *making* of the [work]") (emphasis added).

translational ambiguities in a particular way.³¹⁵ Because the Google Translate users exercise *no* control over how the translation works (i.e., how their general idea, to produce a translation of this Article, becomes a final work), they do not execute the final work and thus cannot claim authorship over it.³¹⁶

Accordingly, one might argue that Paul³¹⁷ is an “ordinary tool” (rather than a “generative machine”) because, at a functional level, Paul does exactly what a camera does: the operator points the machine at a subject, and the machine captures an image of that subject and generates a hard-copy depiction. To be sure, there is a fundamental difference between Paul and an “ordinary” camera: “ordinary” cameras do not contribute any creative content to the images they produce, while Paul’s sketches reflect the aesthetic creativity of the machine’s designer. Cameras are creatively passive—or “essentially completely transparent in conveying the meaning of the [photographer] from author to audience”³¹⁸—and Paul is creatively active: its outputs always reflect the creativity (Tresset’s style) programmed into the machine. Not all cameras, however, are completely passive. Some digital cameras use filters or image-processing technology to add aesthetic elements or simulated objects to photographs in real-time.³¹⁹ At least one camera application allows users to apply a “sketch” filter to their images, to produce a result that looks similar to the drawings that Paul creates.³²⁰ One might argue that such a camera application—which modifies images to look like a hand-drawn sketch or changes the background of an image—is functionally equivalent to Paul. Both produce images that reflect the creative contributions of the designer of the

315. See *Google Translate*, GOOGLE, <https://translate.google.com/> [perma.cc/QH8V-LMR9] (last visited July 31, 2019).

316. Google is similarly not the author of the resulting translation, because while Google’s engineers may be responsible for *how* the algorithm produces the work, these engineers lack any conception of the content of the resulting work. Thus, Google Translate is a “partially generative” machine because it relies on its users to determine its output, and its designers cannot anticipate the outputs. See *supra* Section III.C.1 (discussing the difference between a “fully generative” machine and a “partially” generative machine); *infra* Part IV (discussing the “authorless” work and how automated translations fall into this category).

317. See *supra* notes 268–271 and accompanying text (describing Paul, the generative machine that generates sketches of human subjects in the style of Tresset, Paul’s creator).

318. Boyden, *supra* note 207, at 385.

319. See, e.g., Mallory Locklear, *Snapchat’s new filters make your photo backgrounds look surreal*, ENGADGET (Sept. 25, 17), <https://www.engadget.com/2017/09/25/snapchat-filters-make-backgrounds-look-surreal/> [perma.cc/PRL8-DSGQ] (describing a recently implemented feature of the app Snapchat which “allow[s] [users] to switch the real sky out [of their photographs] for something entirely different including a starry night, a sunset, one with a brewing storm or a sky with rainbows”).

320. See Pixelab, *Sketch Camera*, GOOGLE PLAY APP STORE, https://play.google.com/store/apps/details?id=gr.pixelab.sketch&hl=en_US [perma.cc/MPG2-FX3J] (last visited Mar. 9, 2019) (“Sketch Camera” is an app suitable for photo editing).

tool (the application developer or Tresset) and the user of the tool (who directs the tool towards a particular subject for image capture).

In each of the above scenarios—when a user employs Paul to create a sketch of her friend, when that same user takes a picture of her friend with an ordinary camera, or when she uses a modified camera application to create a sketch-style image of her friend—the user both conceives of the content of the work, and wields the tool under her control. Like the amateur photographer described above, Paul’s user influences both *what* the machine depicts and *how* it will create the image. While the user does not have any influence over Paul’s algorithm, the user contributes acts of execution by framing the subject and by defining compositional elements like the subject’s distance from the camera and the subject’s expression. Two different users who attempt to use Paul to create two identical images of the same human subject (thus acting on an identical *conception*) will produce two different resulting images because of the differences in *how* the user positions the subject in front of Paul’s camera (differences in the *execution*). Therefore, the sketches that Paul produces are works of sole authorship, attributable to the person who employs the machine to create the sketch.³²¹

To be sure, determining whether the user of a machine sufficiently “executed” the resulting work may require some difficult line-drawing. Consider, for example, one of Google’s latest product innovations: an autonomous camera called Google Clips.³²² Clips “is designed to look like a camera” and “has been trained to recognize facial expressions, lighting, framing, and other hallmarks of nice photos” and “familiar faces,” can be “affixed to your jacket, set on a tabletop, carried in your palm or placed anywhere with a view,” and “watches the scene, and when it sees something that looks like a compelling shot, . . . captures a 15-second burst picture.”³²³ The user must simply place Clips in a particular location and activate the device. Is the user’s placement of the camera in a particular location an act of *execution*? The device’s programmers, not the user, are responsible for some of the other elements one typically associates with photographic authorship, such

321. If, instead, Tresset designed his machine to create sketches from uploaded digital image files (rather than from images captured by the machine’s camera), then Paul’s outputs might be “authorless.” The users who supply the image files would not “execute” the works; they have no influence over how Paul converts the image files into sketches.

322. Google, *A new angle on your favorite moments with Google Clips*, KEYWORD BLOG (Oct. 4, 2017), <https://www.blog.google/topics/hardware/google-clips/> [perma.cc/2X3B-9TBU].

323. Farhad Manjoo, *The Sublime and Scary Future of Cameras With A.I. Brains*, N.Y. TIMES, Feb. 27, 2018, <https://www.nytimes.com/2018/02/27/technology/future-cameras-ai-brains.html?smid=pl-share> [perma.cc/46AE-99TG] Clips may present problems similar to those raised by security camera footage. *See supra* note 102.

as lighting, and, crucially, timing. The user does, however, frame and define the potential subjects of the resulting photographs—by placing the camera in a particular location, e.g., a kitchen counter or the handlebars of one’s bicycle, the user essentially “points” the camera at a set of potential subjects. If a user placed the Clips device high atop a ledge in New York’s Grand Central Terminal for 3 hours, Clips might “decide” to take a series of photographs at opportune times, when the lighting was just right, or when the framing of the crowds below made for a compositionally balanced picture. Is such a scenario materially different from a photographer who places an ordinary camera atop the same ledge and instructs it to take photographs at three-minute intervals for three hours? In the latter scenario, one may comfortably say that the photographer is the author of the photographs because she *executed* the pictures (by setting up the camera and setting the shutter timer). But in the former, one might feel less comfortable recognizing the user as an author—she has neither manipulated the camera’s settings (i.e., focus, aperture, or shutter speed), nor is she responsible for the timing of the photograph. “Point and shoot” may together make one an author, but can the same be said about point without shoot?

To answer these difficult questions, one might return to a basic definition of “execution.” To satisfy the execution requirement, the person claiming authorship must be responsible for controlling the basic steps that will lead to the *manifestation of the key expressive elements of the work*. The executional significance of the users’ acts may depend on what exactly is expressive about the resulting work. In other words, the execution inquiry might begin by analyzing what the expressive elements of the work are, and only then proceed to determine who is responsible for the executional acts that led to the creation of those elements. This is the same analysis that allows us to conclude that the user, not the programmer, of a picture produced on Microsoft Paint is responsible for the picture’s execution—while Microsoft Paint’s software developers are certainly responsible for the work’s physical existence (i.e., the effects of the different brush or pencil tools, or the available colors), the *expressive elements* of the work are traceable directly to the user.

Returning to the Clips example: If the photograph’s expressive content is traceable primarily to its placement, i.e., to its positioning on a ledge above a crowded train station, then perhaps the user who placed the camera there *executed* the photograph because her placement was the source of the photograph’s expressive content. But if the photograph’s timing primarily supplies its expressive content, for example, i.e., to the camera’s capturing the

user's infant child's adorable smile, then perhaps the user's claim is weaker.³²⁴ And if the user cannot establish that she executed the resulting image, the user similarly cannot "adopt" the expressive elements of the image as her own. In such a scenario, the image may be "authorless."³²⁵

The following figures summarize the framework discussed above for allocating authorship in machine-enabled works:

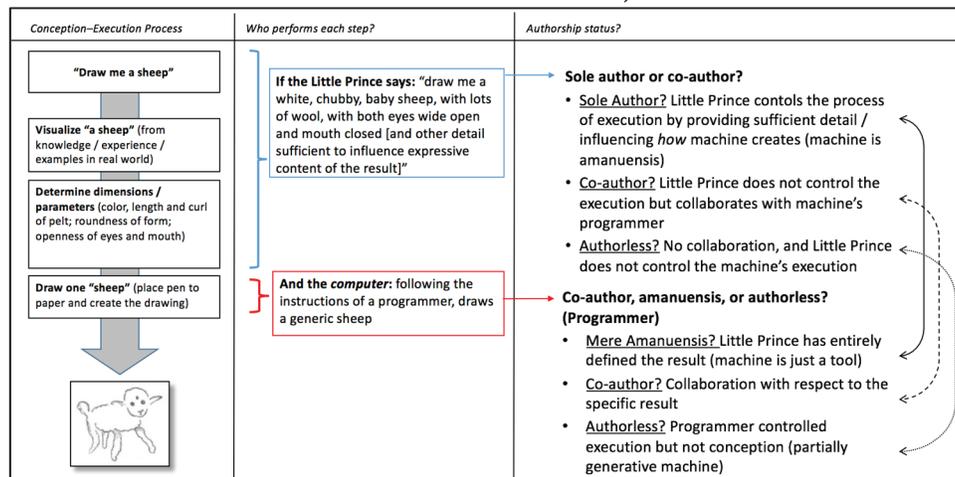
Figure 7: "Draw Me A Sheep" (Example 3: If the Little Prince had provided general instructions to a machine)

Conception–Execution Process	Who performs each step?	Authorship status?
<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">"Draw me a sheep"</div> <div style="text-align: center;">↓</div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Visualize "a sheep" (from knowledge / experience / examples in real world)</div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Determine dimensions / parameters (color, length and curl of pelt; roundness of form; openness of eyes and mouth)</div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Draw one "sheep" (place pen to paper and create the drawing)</div> <div style="text-align: center;">↓</div> 	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;">If the Little Prince says: "draw me a sheep"</div> <div style="border: 1px solid black; padding: 5px;">And the <i>computer</i>: following the instructions of a programmer, draws a generic sheep</div>	<p>→ Not an author (general conception without execution)</p> <p>→ Sole Author or Authorless? (Programmer)</p> <ul style="list-style-type: none"> • <u>Sole author?</u> the machine is "fully generative" (i.e. choose one of 5 farm animals to draw, etc.) → sole author (cf. videogame cases) • <u>Authorless work?</u> the machine is "partially generative," programmer couldn't anticipate what it would be asked to draw then the programmer lacks conception → Work is authorless

324. One might object that this solution is not administrable: how are courts to identify the expressive content of a particular work? While this approach certainly relies on some difficult line drawing, these types of questions are questions of fact and are thus suitable for resolution by judges or juries.

325. We will return to the concept of "authorless" works in the next Section.

Figure 8: “Draw Me A Sheep” (Example 4: If the Little Prince had provided specific instructions to a machine)



IV. THE AUTHORLESS OUTPUT

A. WHAT COMPUTER-ENABLED WORKS ARE “AUTHORLESS”?

Our approach delineates three categories of generative machines. Machines designed to create outputs which reflect *only* the creative contributions of the users are “ordinary” tools, and we should treat them in the same way we treat cameras, word processing programs, and other mechanical or digital adjuncts to the creative process. Machines which, instead, are capable of producing outputs with minimal user input are “fully-generative” in that their outputs necessarily flow from the creative contributions of the machines’ designers—who, accordingly, are the authors of the resulting works, even if someone other than the machine’s designer operates the machine. And machines which produce outputs reflecting the creative contributions of *both* the designer and the user are “partially-generative” in that the machines do not wholly generate the expressive content of the resulting works, but instead rely on the contributions of users.

If the user of the machine supplies her creative contribution without influencing *how* the machine translates that contribution into a final work, then the user does not *execute* the final work and thus cannot claim authorship.³²⁶ And assuming that such a machine is truly “partially-generative”—i.e., that the designer of the machine cannot anticipate the resulting work without any prior knowledge of what the user will input into the machine—the designer of the

326. A person who supplies a fully formed conception, but does not *execute* how that conception comes into physical being, cannot claim authorship over the result. *See supra* notes 81–88 (discussing *Kelley*).

machine may also fail to satisfy the authorship test. This designer might claim to have executed the work, because she defined and controlled the process through which the work came into being. But without being able to anticipate the user's role, the designer cannot claim to have generated a complete creative plan for the work. Therefore, neither designer nor user would have a sufficient authorship claim.

But such a situation does not necessarily result in the work being "authorless." As shown in Part II, creators may combine their individual contributions to create a "joint work" even if their contributions, standing alone, would not rise to the level of authorial contributions.³²⁷ But co-authorship doctrine does not allow for merger standing alone: at least for inseparable joint works,³²⁸ co-authors must, at the time of each individual's creation, be aware of and influenced by each other's specific contributions. And in many cases involving partially-generative machines, the designer of the machine may *not* be aware of the (necessarily asynchronous) contribution of the user.

Therefore, there is a possibility of a set of "authorless" outputs that come into being through the participation of two or more non-collaborating actors, neither of whom have a sufficient claim of authorship. These outputs are not necessarily "machine authored" or "computer generated": as the Article has shown, machines (in their current form) are not capable of authorship.³²⁹ These works are authorless because of the *lack of any author*, not because their authors are machines. Therefore, the existence of a human authorship requirement, often discussed in the literature surrounding computer-enabled works,³³⁰ is irrelevant to the inquiry.

The musical accompaniments produced by Google's A.I. Duet, for example, may be authorless. The designers of the machine, who are fully responsible for training the machine's neural network with musical examples and tuning the algorithm, cannot claim to be the authors of the result because their creative plan for the work is incomplete: they cannot anticipate what the user will input into the program, and therefore the user's creative autonomy disrupts their authorship claim. And the users of the machine do not *execute* the musical accompaniment because the users do not control *how* A.I. Duet

327. See *supra* note 134 (discussing *Gaiman v. McFarlane*, 360 F.3d 644 (7th Cir. 2004)).

328. See *supra* Section II.F.4.

329. See *supra* Section III.A (discussing and rejecting the concept of machine authorship).

330. See, e.g., Bridy, *supra* note 3, at 8 (discussing the human authorship requirement); Clifford, *supra* note 207, at 1682 (same); Miller, *supra* note 25, at 1060–67 (same); Denicola, *supra* note 4, at 265–69 (same).

analyzes the user-supplied melody and produces an accompanying musical line.

Similarly, the translations produced through translation algorithms may be authorless. The designers of the algorithm are responsible for *how* the algorithms convert text from one language to another, but cannot anticipate what the resulting work will be at the time of their participation in the creative process. And the users of the algorithm may supply the text to translate, but they do not influence *how* the algorithm translates the text. No matter how eloquent or accurate the translation, it will lack a human author.

Consider another hypothetical: a newspaper pays a technology company to develop a machine that will convert raw news agency reports into articles reflective of the newspaper's journalistic style.³³¹ The technology company will use the articles in the newspaper's archive to train the machine to emulate the writing style used by the newspaper, enabling the machine to convert a basic report of facts into an article reflecting the newspaper's reportorial and editorial biases.³³² If the editors of the newspaper simply supply the machine with a raw news report they purchase from a news agency, the editors do not control *how* the machine converts that report into the final publishable news article. Thus, the editors are not the authors of the output. Similarly, the programmers who create the machine do not have any conception of the expressive content of the output—it would be impossible for the programmers to anticipate the content of the resulting articles at the time of their participation in the process (i.e., when they program the machine). Unless the programmers and editors collaborate with respect to a specific resulting article (for example, if the programmers built the machine and worked with the editors to process a particular news report into a stylized article), the resulting outputs will be “authorless.”³³³

331. Newspapers often rely on raw news reports from news agencies, like Reuters, to provide the source material for their articles. See Paul Clough, *Measuring Text Reuse in the News Industry*, in *COPYRIGHT AND PIRACY: AN INTERDISCIPLINARY CRITIQUE* 247, 249–50 (Lionel Bently, Jennifer Davis & Jane C. Ginsburg, eds. 2010).

332. Note that this hypothetical is similar, although not identical to, the examples of machine-generated news reports mentioned earlier. See *supra* note 209. The existing examples of machine-generated news reports may not be “authorless” because the users of these machines may exercise control over *how* the machines work, and therefore these users may be conceptually equivalent to the users of sophisticated cameras (who are the authors of the photographs they produce).

333. As noted in note 312, *supra*, the “Next Rembrandt” is an example of a machine-enabled work created through a collaboration involving the designers of the machine and the people who use that machine to create a specific result. Because the scientists and art historians

Finally, consider the popular music service Pandora.³³⁴ Users of Pandora create “stations” by providing Pandora with an artist, song, or composer whose music they enjoy. Pandora then generates a playlist of songs related to the users’ input, and allows users to indicate whether they approve or disapprove of each song Pandora selects. Pandora’s algorithm “crunches users’ interests” to learn about each user’s preferences, and uses the resulting knowledge to improve the playlists it generates.³³⁵ Because the users do not control *how* Pandora processes their inputs (and because Pandora adds to those inputs by supplementing expressed user preferences with preference-predictive selections), the users are not the “authors” of the resulting playlists.³³⁶ And Pandora’s programmers, the most intuitive candidates for playlist authorship, do not have any conception of what the playlists will contain when they program the algorithm. Therefore, the resulting playlists’ selection and arrangement of recorded performances, though they may resemble copyrightable compilations, are “authorless.”

At first blush, the concept of an “authorless” output may seem novel—these products appear to possess sufficient “originality” to fall within the domain of copyright. But the *process* of creation, and not just the *result*, is relevant to the authorship inquiry.³³⁷ Works like Chapman Kelley’s *Wildflower*

who created the “Next Rembrandt” collaborated with each other, the resulting painting is not “authorless.”

334. PANDORA, <https://www.pandora.com/> [perma.cc/Z8CX-XA2Y] (last visited July 31, 2019).

335. Tyler Gray, *Pandora Pulls Back the Curtain On Its Magic Music Machine*, FAST COMPANY (Jan. 21, 2011), <https://www.fastcompany.com/1718527/pandora-pulls-back-curtain-its-magic-music-machine> [perma.cc/PX3B-WUPQ].

336. To be clear, the playlists may be copyrightable (if sufficiently authored) as a compilation. See 17 U.S.C. § 103 (2018) (“The copyright in a compilation . . . extends only to the material contributed by the author of such work, as distinguished from the preexisting material employed in the work, and does not imply any exclusive right in the preexisting material.”); § 101 (defining “compilation” as “a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship”). The copyrightability of music playlists is uncertain. See Marc A. Fritzsche, *Copyrightability of Music Compilations and Playlists: Original and Creative Works of Authorship?*, 6 PACE INTELL. PROP. SPORTS & ENT. L.F. 258, 260 (2016) (noting that in the U.S., “it remains uncertain whether the act of compiling songs or arranging a playlist fulfills” the basic criteria of originality set out in *Feist Publ’ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991)). However, we assume that the playlists are copyrightable as compilations for the purposes of this argument.

337. See Ralph D. Clifford, *Random Numbers, Chaos Theory, and Cogitation: A Search for the Minimal Creativity Standard in Copyright Law*, 82 DENV. U. L. REV. 259, 271–72 (2005) (noting that “[i]n addressing copyrights and whether sufficient intellectual creativity is contained within the work, the primary focus should be on the product, although the process used to

Works and Kurant's termite mounds³³⁸ may be "authorless" not because the *product* falls outside the subject matter of copyright, but because the *process* behind their creation was not sufficiently authorial.³³⁹

One might argue that copyright authorship doctrine should evolve in order to allow this class of machine-enabled "authorless" outputs to come within the scope of copyright. In the next Section, we investigate potential revisions to copyright doctrine that would permit the more relaxed definition of authorship necessary to include "authorless" machine-enabled outputs within the scope of copyright.

B. REEXAMINING AUTHORSHIP DOCTRINE TO AVOID THE CLASSIFICATION OF MACHINE-ENABLED OUTPUTS AS "AUTHORLESS"

As shown in Section IV.A, a machine-enabled output will be authorless when: (i) The designer of the machine, who programs and trains the machine and thus is responsible for *how* the machine executes its third party-given task, lacks adequate *conception* of the resulting output; (ii) the user of the machine, who employs the machine to produce the output, lacks any control over *how* the machine works, and thus lacks any role in the resulting work's *execution*; and (iii) the designer of the machine and the user of the machine are not co-authors because they have not contemporaneously collaborated to produce the output. Rather, the designer of the machine neither knows who the user is, nor what task she will assign the machine, and the user, once she has assigned the task, has no influence over its execution. This Section will investigate whether we might narrow or eliminate the class of machine-enabled "authorless" outputs by reinterpreting copyright doctrine to relax the requirements of authorship or co-authorship. This Section does not presume that such a reinterpretation is necessary or desirable—instead, this Section examines whether the Copyright Act *permits* relaxing authorship criteria. Consistently with the 1976 Copyright Act's "unifying theme" of technological neutrality,³⁴⁰ any reinterpretations of

produce the work is also relevant" and that "[i]f only the product is examined with no examination of methodology of production, it will prove impossible to separate human-generated creative works from those generated by sophisticated computer programs based on autonomous artificial intelligence techniques"). *Cf.* Denicola, *supra* note 4, at 273 ("[A] work's contribution to the public welfare does not seem dependent on the process that produced it.").

338. *See supra* Section II.C (discussing Agnieszka Kurant's art comprised of colored termite mounds).

339. *See supra* notes 81–88 (discussing *Kelley v. Chicago Park District*, 635 F.3d 290 (7th Cir. 2011)).

340. 4 NIMMER ON COPYRIGHT § 12A.16(b), *supra* note 5.

authorship doctrine must apply equally in the traditional and generative-machine contexts.

If the outputs of partially-generative machines did qualify as “joint works,” they would fall into the category of “inseparable” joint works because the contributions of the machine’s user and designer cannot be disaggregated into individual expressive contributions.³⁴¹ This Article’s earlier exploration of joint works in Section II.F suggests that Congress lacked any specific intent regarding *non-collaboratively* created inseparable joint works, largely because it is unlikely to have imagined such creations.³⁴² However, partially-generative machines offer the possibility of asynchronous combinations of sub-copyrightable contributions into inseparable works.³⁴³ In assigning the machine a task, the user may be contributing no more than ideas, and the machine designer’s contribution represents neither a “work” nor sub-copyrightable components (because it exists only in latent form).³⁴⁴ If Congress did not anticipate “inseparable” joint works produced through a combination of non-copyrightable contributions of multiple unacquainted co-authors, might the definition of joint works nonetheless encompass them?³⁴⁵ The

341. See *supra* note 133 and accompanying text (defining “inseparable” joint works as works which cannot be disaggregated into individual component parts).

342. See *supra* Section II.F.2 (suggesting that examples of non-collaboratively produced inseparable joint works were rare, and perhaps impossible, before the introduction of sophisticated generative machines).

343. While in the “analog” world, asynchronous creation by definition would require the individual contributors to supply independent and distinct contributions to a joint work, which could then be merged into an “interdependent” whole. See *id.*

344. Note, however, that in the “partially-generative” machine context, the machine’s designer will be unable to claim sole authorship because the machine’s production of an output will depend on a user’s input of some creative contribution that the designer could not have anticipated. If the machine’s production of an output does *not* depend on the user’s input of some creative contribution—if the machine is capable of producing a work at the push of a button, or after the user has chosen among a set of limited parameters—then the machine, like Harold Cohen’s AARON, is “fully-generative” and the machine’s output is a work of sole authorship attributable to the machine’s designer. See *supra* Section III.C.1 (discussing the difference between fully- and partially-generative machines). The same analysis would apply in the traditional context: for example, the author of the Choose Your Own Adventure books remains the sole author despite offering readers choices about how to arrange the plot elements.

345. In other words, might the 1976 Act’s definition of joint works to exclude works created by multiple creators who are unacquainted with one another apply only to joint works of the “interdependent” variety?

unacquainted participants do, after all, intend to merge their contributions, through the aid of the machine, into a “unitary whole.”³⁴⁶

In support of that contention, the policies against recognizing noncollaborative joint works evoked in Section II.F do not apply to inseparable machine-enabled authorless works.³⁴⁷ Extending co-authorship to two sequential contributors who are “strangers to each other” would not allow the second author to lay claim to a pre-existing work (because there is no pre-existing work). For the same reason, denying co-authorship to asynchronous unacquainted contributors would not leave each contributor with separately copyrightable contributions to fall back on. Rather, unless Congress revisits concepts of joint authorship in order to allow protection for inseparable contributions by asynchronous unacquainted contributors, then many machine-enabled outputs will not be works of authorship at all.

This enlargement of the universe of co-authors would narrow (but not eliminate) the class of “authorless” computer-enabled works; as long as the user contributed some copyrightable expression, the user and the designer could be co-authors (one supplying the detailed conception, the other supplying the execution, respectively) even if they were “strangers to each other.” If the statutory definition can embrace both asynchronous intent and ignorance of fellow contributors, then the machine’s programmers and data trainers might qualify as one half of the co-authorship equation, for they intend for unknown future users to employ the machine to produce whatever outputs it enables. The users will not have encountered the programmers and data trainers, and may assign tasks to the machine long after the latter have prepared the machine for others’ use, but if the users’ definition of the task transcends a mere command (“Draw me a sheep!”) and furnishes adequate expressive details (elaborated characteristics of the sheep to be drawn), then they might constitute the other half of the equation, since their employment of the machine manifests their intent to merge their contributions with those of the upstream contributors.

346. Of course, if the contributions must be independently copyrightable, as some Circuits require, few if any outputs of partially-generative machines could be considered joint works. See authorities cited *supra* note 185.

347. See *supra* Section II.F.3 (noting that the 1976 Act’s legislative repeal of the Second Circuit cases like *Marks* and *12th Street Rag* was motivated by a desire to prevent later authors from “bootstrapping” an ownership stake in a previously created work by claiming that her contribution combined with the existing work to form a “joint work,” and noting that Congress’s post-1976 Act rule did not cause works to fall outside of copyright because each asynchronous creator could claim sole authorship in her individual contribution).

1. *Joint Authorship*

Interpreting the statutory definition of joint works to encompass non-collaborative contributions that produce an inseparable unitary whole will not entirely eliminate the class of “authorless” machine-enabled outputs. When creative participants work together to combine individually unoriginal contributions, their collaboration can endow the whole with originality that the parts lacked.³⁴⁸ But if collaboration supplies the alchemy that turns the combination into authorial precious metal, then absent collaboration, the individual contributions remain uncopyrightable dross. For example, if a user employs a partially-generative machine to create a work, but the user supplies little more than an unprotectable idea to the machine (i.e., “draw me a sheep” or “translate this text from the German”) then the user cannot be considered an author (even a co-author) because that user’s contribution does not set out a creative plan, and because “collaboration” requires more than merely issuing a command.

Suppose, however, that user follows up her initial command by “tweaking” the results. Like the Little Prince, who rejected the aviator’s initial sheep sketches, suppose the user specifies her dissatisfactions with each output and keeps “sending the machine back” to redo the drawing until it produces an image that corresponds to the user’s wishes (wishes that may have evolved during the process of image elaboration).³⁴⁹ In the traditional context, this interaction between the Little Prince and the aviator might suffice to make the former a genuine collaborator, rather than a mere idea-proposer.³⁵⁰ The final drawing will inseparably merge the pair’s contributions. But the peremptory Prince and the long-suffering aviator both are acquainted (though the acquaintance arises from the encounter in which the Little Prince issues his commands) and contemporaneously work together to satisfy the Prince’s demands. Moreover, no matter whether the Little Prince’s interventions make him a co-author, the aviator’s authorship remains a constant.

348. See discussion *supra* Section II.F.5.

349. The process described here differs from the relationship of Calder and his welders, *see supra* notes 118–120 and accompanying text, because Calder there provided two-dimensional sketches documenting the intended sculpture.

350. But maybe not: for example, case law generally rebuffs the authorship pretensions of architects’ clients who claim co-authorship because they instructed the architect to change the location of the stairs or the closets. *See Meltzer v. Zoller*, 520 F. Supp. 847, 857 (D.N.J. 1981) (holding a plaintiff who had commissioned an architect to design a home, and who had “contributed ideas and made certain changes” to the home’s design, was not the “author” of the resulting design because “consultation between client and architect, including . . . coordination of the client’s desires in the plans, is typical in the architectural profession”).

In situations involving partially-generative machines, the task-assigning user's reiterative issuance or refinement of her instructions to the computer function similarly to the Little Prince's orders, but the analogy to the traditional context otherwise falls short. Here, the user is not acquainted with the programmers and data trainers behind the machine, nor are they contemporaneously working together to satisfy the user's demands. Moreover, while the aviator's authorship of his drawing, with or without the Little Prince's continued input, is not in question, it is not at all clear, for the reasons explored in Part III, that sole or partial authorship of the machine-enabled output can be attributed to the programmers and data trainers. As a result, the machine (or, more correctly, the upstream humans behind it) does not provide an expressive contribution with which the user can merge her arguably expressive input. If neither participant supplies sufficient copyrightable expression, their combination would be copyrightable only if we characterized the iterative process as a collaboration adequate to transform otherwise uncopyrightable inputs into a copyrightable "unitary whole."³⁵¹ If the programmers have designed the machine to respond to the user's sequential demands, even though the user does not interact with the programmers, can we call the output the result of a "collaboration"?³⁵²

To characterize the user's repeated interaction with the machine as a kind of virtual collaboration between the user and the machine's designer strains the 1976 Act's assumptions regarding not only the temporal but also the expressive dimensions of the contributors' interactions. "Collaboration" implies more than the "back and forth" of the iterative process that a "tweakable" program implements; collaborators influence each other's contributions.³⁵³ Even if one participant does not rewrite another's contribution, each participant modifies (or at least considers modifying) her own contribution in light of her co-authors' perceptions, suggestions, or objections. By contrast, a partially-generative machine's recurrent prompts may orient the user's choices, but nothing the user does can alter the pre-

351. *See supra* notes 183–184 and accompanying text (arguing that collaboration transforms insufficient contributions into those capable of supporting the claim of co-authorship).

352. Even if one entertained the possibility that asynchronous contributions might form a joint work so long as each participant intended "at the time [each] writing is done" that his or her contributions would be merged into a unitary whole, the partially-generative machine scenario goes a step farther: the contributors neither decide simultaneously to merge independently expressive contributions (to form an "interdependent" joint work), nor do they work together at the same time to create an expressive work (to form a "inseparable" joint work). The scenario thus corresponds to neither of a coauthor's traditional salient acts.

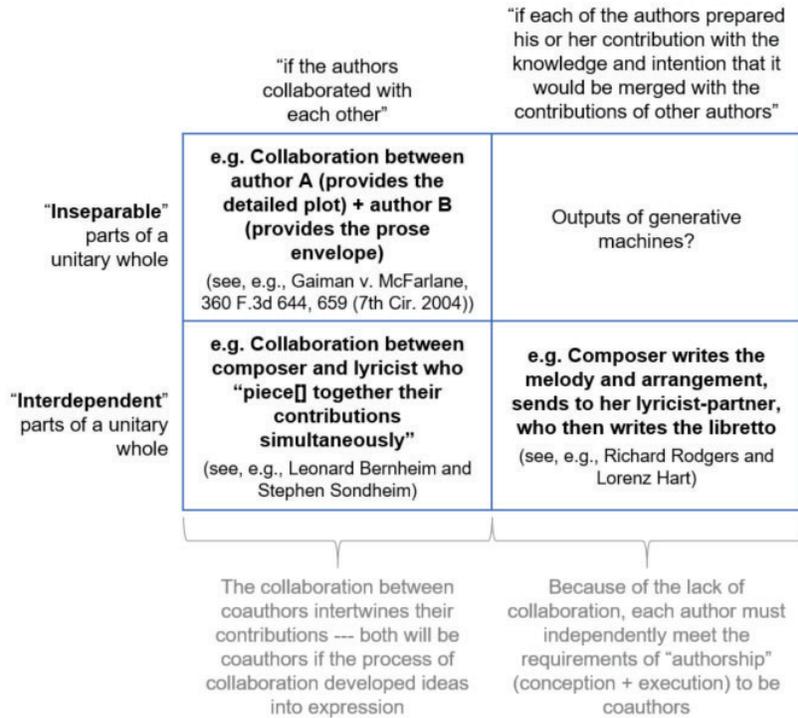
353. *See supra* Section II.F.5 (noting that collaboration implies an intertwining of each contributor's contribution).

determined options the computer offers the user. The user's relationship to the machine resembles that of the reader of a "Choose your own adventure" story. The reader may at multiple points select from among a variety of story lines, but the resulting tale remains confined to the range of possibilities contained within the book.

If one cannot characterize the coordinated creation of an output by the designer of a machine and its user as "collaboration," then both participants necessarily lack the requisite elements of "authorship" if neither has both conceived of and executed the work. It is therefore unlikely that the 1976 Act welcomes interpreting its definition of joint works to encompass the inseparable combination of unacquainted persons' asynchronous non-copyrightable contributions (virtual or otherwise).³⁵⁴

354. Moreover, recognizing joint authorship between machine designers and machine users may create administrability problems. Finding joint authorship would mean that both the designer and the user could unilaterally grant non-exclusive licenses to third-parties for the exploitation of the work. *See* *Davis v. Blige*, 505 F.3d 90, 100 (2d Cir. 2007) ("A co-owner may grant a non-exclusive license to use the work unilaterally, because his co-owners may also use the work or grant similar licenses to other users and because the non-exclusive license presumptively does not diminish the value of the copyright to the co-owners."); *Meredith v. Smith*, 145 F.2d 620, 621 (9th Cir. 1944) (noting that a "co-owner would have had the right to give permission" for nonexclusive use of a copyrighted work). But a co-owner of copyright who grants a non-exclusive license "is accountable to his co-owner for income gained by the grant of the license." *See* *Davis*, 505 F.3d at 100. Therefore, if the machine's user is a co-author, then (absent a contractual arrangement with the designer-coauthor) she may not grant a non-exclusive license to use the resulting work without providing compensation to the designer-coauthor. Moreover, neither co-author may grant exclusive licenses to exploit the work without the consent of the other co-author(s). *See id.* at 101 ("[A] co-owner cannot unilaterally grant an exclusive license."). However, many of these issues could be resolved by a license agreement between the machine's designer and user. *Cf.* *Miller*, *supra* note 25, at 1059 (noting that "the employment relationship and bargaining among the interests involved" may solve difficult problems arising from the unclear apportionment of ownership of copyright in computer-generated works).

Figure 9: Absent collaboration, designer and user must each meet the authorship requirements independently



2. Sole Authorship

For some commentators, in any event, joint works status would not suffice; they would go farther to argue that the user of a generative machine is the *sole* "author" of the resulting work, even if that user contributes very little to the conception and execution of the work.³⁵⁵ But as we have noted, copyright doctrine is technologically neutral,³⁵⁶ denominating the user who

355. Denicola, *supra* note 4 at 284 ("If computer-generated works . . . are owned by someone other than the user of the computer—or are not copyrightable at all—it becomes necessary to distinguish situations where the computer is merely a tool of a human creator from those where the computer is itself the creator. This is an obviously difficult, indeed indeterminate, and ultimately pointless endeavor."); *id.* at 286–87 (concluding that "[a] computer user who initiates the creation of computer-generated expression should be recognized as the author and copyright owner of the resulting work?"); *see also* Samuelson, *supra* note 206, at 1200–04, 1227–28 (1986) (noting that even though the user may not have contributed sufficient authorship under traditional copyright analysis, policy reasons favor granting authorship to the user who is the "instrument of fixation for the work, that is, the person who most immediately caused the work to be brought into being").

356. 4 NIMMER ON COPYRIGHT § 12A.16(b), *supra* note 5.

merely supplies an idea or a command an “author” would produce anomalous results in the traditional copyright world. Consider the following:

- If X asked Y (a human) to produce a poem in iambic pentameter about the moon, Y would be considered the sole author (assuming the work for hire doctrine does not apply) of the resulting poem because X has supplied no expressive elements.
- But if X asked Z (an algorithm) to produce a poem in iambic pentameter about the moon, X would be considered the author-in-fact, even though X provided no more expression here than she communicated to Y.³⁵⁷

Vesting authorship in the task-assigner not only would sidestep the requirement that authors contribute “expression,” and not merely “ideas” (i.e., that they furnish an elaborated *conception*); it would also forego the requirement that authors control the process of *execution*. As we have seen, a task-assigner who does no more than give a command does not intervene in the actual production of the output; he leaves it to another human being (for example, the Little Prince’s aviator) or to the machine to make all creative choices within the broad contours of the command. But if a user who did not control a generative machine (because that user had no influence over *how* the machine produced its outputs) nonetheless could be the author of the output, then that result would clash with decisions such as *Kelley v. Chicago Parks District*, in which Kelley’s authorship claim failed because he did not control the random forces to which the court attributed the work’s sole execution.³⁵⁸

Therefore, even if authorship claims did not require actual collaboration among an alleged joint work’s participants, relaxing that co-authorship criterion would not suffice to anoint authors of many machine-enabled outputs. To achieve that end, it would also be necessary either to abandon the hallmarks of authorship in the traditional copyright world, or to rescind the fundamental principle of technological neutrality in order to create specific rules for machine-enabled authorship.³⁵⁹ Because Congress has repeatedly

357. For example, if the Google Translate user were considered the author of the resulting translation, then such a user would earn authorship simply by supplying a basic idea (i.e., translate this text into Spanish).

358. See *supra* notes 81–88 (discussing *Kelley v. Chicago Park District*, 635 F.3d 290 (7th Cir. 2011)).

359. For an argument that technological neutrality is a misguided policy, see generally Greenberg, *supra* note 1 (questioning “the expedience of technological neutrality as embodied by the 1976 Copyright Act” and arguing that technology neutrality is “both suboptimal and often self-defeating” and that “technological discrimination, a combination of neutrality and specificity, can better serve broader copyright and innovation policy goals”).

affirmed its policy that basic copyright rules continue to apply to new technological environments,³⁶⁰ however, this Article does not advocate technologically variable standards of authorship in order to allow that which fails to satisfy the traditional copyright goose to suffice for the generative-machine gander.

V. CONCLUSION: IF NOT COPYRIGHT, THEN WHAT?

This Article has identified four ways to allocate authorship when individuals use machines to create works. First, and most commonly, one might attribute sole authorship to the user of the machine.³⁶¹ If a creator utilizes a passive machine—call it an “ordinary tool”—whose designer does not creatively contribute to the content of the resulting work, then that creator-user is necessarily the only author of the work produced through the aid of that machine. In these circumstances, “it is . . . the thought of the artist [—and *only* the artist—] which directs the instrument, which guides and inspires the material means” through which the work comes into being.³⁶² Therefore, there is no cause to doubt the claim of authorship—even though “the [camera] takes the place, though not entirely, of hand labor,” “it leaves to the artist, to its fullest extent, the labor of the mind.”

Second, if a person builds a machine capable of producing outputs without any creative contributions supplied by the machine’s user or operator, then the designer of such a machine is the author of the machine’s outputs.³⁶³ There may be multiple people involved in the construction of these “fully-generative” machines—engineers, coders, and data trainers, for example—but the “designer” of the machine and the author of the resulting output is the

360. *See, e.g.*, 17 U.S.C. § 102(a) (2018) (“Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, *now known or later* developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.”) (emphasis added); § 101 (defining “[t]o perform or display a work ‘publicly’” to include the transmission of “a performance or display of the work . . . *by means of any device or process*”) (emphasis added); H.R. REP. NO. 94-1476 (noting that 17 U.S.C. § 106 incorporates the technology-neutral definitions in 17 U.S.C. § 101 to avoid “confining the scope of an author’s rights on the basis of the present technology”) (quoting STAFF OF THE H. COMM. ON THE JUDICIARY, 89TH CONG., COPYRIGHT LAW REVISION, PART 6: SUPPLEMENTARY REP. OF THE REGISTER OF COPYRIGHTS ON THE GEN. REVISION OF THE U.S. COPYRIGHT LAW: 1965 REVISION BILL 14 (Comm. Print 1965)); Greenberg, *supra* note 1 at 1514 (“Among numerous radical changes that Congress adopted in the 1976 Copyright Act was the principle of technological neutrality.”).

361. *See supra* Section III.B.1 (discussing “ordinary tools”).

362. Pouillet on Photography, *supra* note 35.

363. *See supra* Section III.B.2 (discussing “fully-generative” machines).

individual (or set of individuals) who endowed the machine with the training and the creative raw material requisite to the machine's generation of a "creative" output.

Third, if the machine in question is "partially-generative"—that is, the machine's outputs reflect the creative contributions of both designer and user—then works produced through the use of the machine may be "joint works" if the designer and user collaborate with each other to create the specific result.³⁶⁴

But, fourth, if the designer and the user do not collaborate with respect to a specific result—for example, if the designer builds and trains the machine and then sells or licenses it to a user, who employs it without the designer's involvement—and neither contribute expression sufficient to form an "original work of authorship," then the resulting output may be "authorless."³⁶⁵

A machine-enabled output will be "authorless" under the following conditions. First, the designer of the machine cannot claim sole authorship of the work. If, however, the designer of the machine can anticipate what the user will do to coax an output out of the machine (for example, if the user has only a limited set of options or parameters to choose from), then the machine is "fully generative" and the designer is the author of the output.³⁶⁶ Second, the user of the machine does not control the machine's executional process. If the user controls *how* the machine works—rather than simply designating *what* the machine produces—then the machine is just an "ordinary tool" and the user is the sole author of the resulting work because she both *conceived* of the work and *executed* it.³⁶⁷ Lastly, the designer of the machine and its user do not actually collaborate in real time with respect to the specific work in question.

If a work meets the above criteria, then the work in question is "authorless" even if the work appears indistinguishable from other works which fall under the protection of the Copyright Act. Because no human participant would meet the requirements of "authorship," and because the contributors to the work's creation cannot claim to be collaborative co-

364. See *supra* Section II.F.5 (discussing co-authorship doctrine as applied to the generative-machine context). For example, the scientists and art historians behind the "Next Rembrandt" collaborated closely to both create the generative machine and use the machine to create their new Rembrandt. See Nudd, *supra* note 213.

365. See *supra* Section IV.A (discussing "authorless" works).

366. See *supra* Section III.C.1.c (discussing the distinction between fully- and partially-generative machines).

367. See *supra* Section III.C.2 (discussing the execution element and machines which may be partially-generative).

authors, the work is not a “work of authorship” and thus falls outside of copyright’s domain.³⁶⁸

This analysis of non-copyrightability may provoke dissatisfaction. After all, if only the *process* through which these otherwise indistinguishable works come into being renders them “authorless,” it seems anomalous to treat apparently identical works so differently. One might therefore argue that if the copyright law cannot deem these authorless outputs true works of authorship,³⁶⁹ then Congress should provide some copyright-like protection notwithstanding the lack of an author.³⁷⁰ What would be the theoretical basis for a copyright-like regime? Any justification for full or partial copyright protection must rely on instrumentalist theories of intellectual property.³⁷¹ (Copyright’s other theoretical prong, the natural or personality rights of the author,³⁷² cannot apply if there is no author.) Instrumentalists might argue that without copyright-like protection, there exist no incentives for machine-creators and

368. See 17 U.S.C. § 102(a) (2018) (“Copyright protection subsists . . . in original works of authorship.”).

369. For arguments that these outputs should be treated as works of authorship, see, e.g., authorities cited in *supra* note 355.

370. See, e.g., Sam Ricketson, *The 1992 Horace S. Manges Lecture: People or Machines: The Berne Convention and the Changing Concept of Authorship*, 16 COLUM. J.L. & ARTS 1, 36–37, 38 (1991) (arguing against the degradation of the human-centered philosophy of authorship, and suggesting that producers might “obtain strong and effective protection under a neighboring rights or *sui generis* regime”); McCutcheon, *supra* note 122, at Part VIII (2013) (suggesting a *sui generis* regime for protection of “authorless” computer-generated works); see also Ramalho, *supra* note 229, at 21–22 (arguing that the outputs of artificially intelligence machines which lack a human author should fall into the public domain, but advocating for the establishment of a “disseminator’s right” to “incentivize” those “who disseminate AI creations” similar to the publisher’s right in the publication of previously unpublished works in the EU).

371. See Rebecca Giblin, *A New Copyright Bargain? Reclaiming Lost Culture and Getting Authors Paid*, 41 COLUM. J.L. & ARTS 369, 373 (2018) (“Instrumentalist theories justify copyright as a way of achieving social and economic aims, putting the public interest at the forefront. [By contrast,] [n]aturalist approaches assume that authors’ contributions of intellectual labor or personality give rise to rights to rewards in their own right (and arguably above and beyond the amount necessary to incentivize the work).”).

372. See, e.g., ROBERT MERGES, JUSTIFYING INTELLECTUAL PROPERTY 150–53 (2011) (arguing that “efficiency is not capable of serving as a stand-alone foundation for IP rights”); Justin Hughes, *The Philosophy Of Intellectual Property*, 77 GEO. L.J. 287, 330 (1988) (describing the “personality justification” for intellectual property, which “posits that property provides a unique or especially suitable mechanism for self-actualization, for personal expression, and for dignity and recognition as an individual person” and noting that according to this theory, “an idea belongs to its creator because the idea is a manifestation of the creator’s personality or self”); Edwin C. Hettinger, *Justifying Intellectual Property*, 18 PHIL. & PUB. AFF. 31, 51 (1989) (“Natural rights to the fruits of one’s labor are not by themselves sufficient to justify copyrights . . . though they are relevant to the social decision to create and sustain intellectual property institutions.”).

machine-users to invest time and effort in the production of outputs. And without proper incentives, society at large might be deprived of outputs from which it might otherwise derive great and lasting value.

But we should not assume that we need copyright-like protection to stimulate the production of authorless outputs. Absent an author, the premise underlying incentive justifications requires substantiation. One must inquire whether these outputs in fact need the impetus of exclusive rights, or if sufficient incentives already exist, for example higher up the chain, through copyright or patent protection of the software programs, patent protection of the specialized machinery to produce different kinds of outputs, and copyright protection of the database the software consults. Trade secrets and contracts may also play a role in securing the outputs.

That said, these forms of protection lack something that copyright—or a *sui generis* regime for the protection of authorless outputs—would provide: protection directly against copying of the outputs by parties not in privity with the designers or users of the machines. The copyright alternatives this Article has evoked may control *access to the machine*, but will not control third-party *access to the output* created by the machine. In other words, while patent or software-copyright protection might protect against copying a firm's means of producing the output, and trade secret or contract law might constrain a firm's customers' exploitation of the outputs, only copyright-like protection protects the outputs themselves from third-party copying.³⁷³

The need for copyright-like protection will depend on an analysis of the type of output in question. For example, there may not be an autonomous market for outputs which derive their commercial value from customization (such as bespoke computer-generated music designed to match the narrative peaks and troughs of a film). As to these outputs, extant intellectual property protections of the upstream process and its components may suffice. But commercially free-standing outputs whose value derives from their content (such as computer-generated news reports) may face a high risk of unauthorized third-party exploitation; perhaps their commercial viability depends on some form of copyright-like protection. We can conjure up a variety of scenarios supporting or debunking the call for *sui generis* protection, but without empirical evidence, it would be imprudent (and premature) to seek to design a regime to cover authorless outputs.

373. The producer of the outputs might employ technological protection measures to discourage copying, but the law will not prevent the “hacking” of these safeguards because 17 U.S.C. § 1201 protects only against circumvention of measures that protect “a work protected under this title.” Authorless outputs are not “original works of authorship” protected under Title 17.

LEGALLY COGNIZABLE MANIPULATION

Ido Kilovaty[†]

ABSTRACT

Swaths of personal and nonpersonal information collected online about Internet users are increasingly being used in sophisticated ways for online political manipulation. This represents a new trend in the exploitation of data, where instead of pursuing direct financial gain based on the face value of the data, actors engage in data analytics using advanced artificial intelligence technologies that allow them to more easily access individuals' cognition and future behavior. Although in recent years the concept of online manipulation has received some academic and policy attention, the desirable relationship between cybersecurity law and online manipulation is not yet fully explored. In other words, regulators and courts have yet to realize the importance of linking cybersecurity law to individual autonomy, privacy, and democracy.

This Article provides an account of the desirable relationship between cybersecurity law and other values, such as autonomy, privacy, and democracy, by looking at the phenomenon of online manipulation achieved through psychographic profiling. It argues that the volume, efficacy, and sophistication of present online manipulation techniques pose a considerable and immediate danger to autonomy, privacy, and democracy. Internet actors, political entities, and foreign adversaries carefully study the personality traits and vulnerabilities of Internet users and, increasingly, target each such user with an individually tailored stream of information or misinformation with the intent of exploiting the weaknesses of these individuals. This Article makes a broader argument about cybersecurity law and its narrow focus on identity theft and financial fraud. Primarily, this Article looks at data-breach notification law, a subset of cybersecurity law, as reflective of that limited scope. It argues that data-breach notification law could provide a much-needed backdrop for the challenges presented by online manipulation, while alleviating the sense of lawlessness engulfing current misuses of personal and nonpersonal data. At the heart of this Article is an inquiry into the expansion of dated notions of cybersecurity law.

DOI: <https://doi.org/10.15779/Z38T727G4R>

© 2019 Ido Kilovaty.

[†] Frederic Dorwart Endowed Assistant Professor of Law, University of Tulsa, College of Law; Cybersecurity Policy Fellow, New America; Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School; Affiliated Fellow, Information Society Project, Yale Law School. I wish to personally thank Claudia Haupt, Andrea Matwyshyn, and Robert Spoo for their guidance and support, the members of the Berkeley Technology Law Journal for their meticulous and thorough work on this Article, the organizers and participants of the 2018 Northeast Privacy Workshop and Ohio State University Center for Ethics and Human Values COMPAS Conference on Targeting with Big Data for their helpful feedback. I'm indebted to the College of Law at the University of Tulsa for its generous summer research stipend to support this project.

Presently, cybersecurity law's narrow approach seeks to remedy materialized harms such as identity theft or fraud. This approach contravenes the purpose of cybersecurity law—to create legal norms protecting the confidentiality, integrity, and availability of computer systems and networks. If cybersecurity law seeks to protect individuals from the externalities of certain cyber risks, it needs to recognize emerging threats targeting computer systems and networks, and subsequently, individual autonomy, privacy, and democracy.

TABLE OF CONTENTS

I.	INTRODUCTION	451
A.	CYBERSECURITY & DATA-BREACH NOTIFICATION LAW	454
B.	BIG DATA & MANIPULATION	455
C.	INFORMATION FIDUCIARIES	457
II.	ONLINE MANIPULATION AND PSYCHOGRAPHIC PROFILING.....	461
A.	PSYCHOGRAPHIC PROFILING AS MANIPULATION	465
B.	THE WRONGFULNESS OF ONLINE MANIPULATION	468
	1. <i>Autonomy</i>	469
	2. <i>Experimentation</i>	473
C.	THE EXCEPTIONALISM OF ONLINE MANIPULATION	475
III.	DATA-BREACH LAW: SILVER LININGS AND GAPS	478
A.	DEFINITIONAL BOUNDARIES	481
	1. <i>Personal: Demographic Versus Psychographic</i>	481
	2. <i>Breach Versus Unauthorized Acquisition</i>	483
B.	SUBSTANTIVE SHORTCOMINGS	486
	1. <i>Identity Theft Versus Manipulation Harm</i>	487
	2. <i>Other Harms</i>	488
IV.	DATA-BREACH NOTIFICATION LAW AS AUTONOMY- BREACH LAW.....	490
A.	REDUCING INFORMATION GAPS	492
B.	INDIRECT REGULATION OF DATA COLLECTION	494
C.	REMEDYING VICTIMS OF MANIPULATION	497
D.	REGULATORY OVERSIGHT	497
E.	MANIPULATION AND THE FIRST AMENDMENT.....	499
V.	CONCLUSION.....	501

I. INTRODUCTION

The landscape of data breaches and personal information misuse is changing. Malicious actors are constantly seeking more efficient, sophisticated, elusive, and low-risk methods of exploiting our data.¹ Surely, the traditional

1. This notion is directly tied to the “accepted wisdom” that in cyberspace, attackers always have the advantage and are constantly able to overcome new defense techniques. *See, e.g.,* David T. Fahrenkrug, *Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy*, in NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, 4TH INTERNATIONAL

form of data breaches is still taking place as it has been for the last two decades. Databases are being constantly hacked and their data exfiltrated, to subsequently be exploited or sold.² The proliferation of data breaches has created the perception, which became a slogan, that it is not a question of “if you will get breached” anymore, but rather “a question of when.”³ These financial-facing forms of data breaches, often resulting in identity thefts and fraud, are still taking place today.⁴ Indeed, most litigation in that context is due to credit card information theft.⁵

Yet, recent scandals surrounding alleged digital interferences in elections and referendums throughout the world suggest that personal and nonpersonal information obtained in data breaches may facilitate a new form of harm. These scandals illustrate that perpetrators may use personal information not only for direct financial gain, as they did for more than two decades, but also for the largely unanticipated political manipulation and direct microtargeting of the data subjects.⁶ This poses the question: what is the role of cybersecurity law today, given these new threats? Do the governing definitions, scopes, and conceptions of cybersecurity law comport with today’s threats?⁷ This Article

CONFERENCE ON CYBER CONFLICT. PROCEEDINGS 2012 197 (C. Czosseck et al. eds., 2012).

2. See Lily Hay Newman, *If You Want to Stop Big Data Breaches, Start with Databases*, WIRED (Mar. 29, 2017), <https://www.wired.com/2017/03/want-stop-big-data-breaches-start-databases/> [perma.cc/6MHD-BYSZ] (noting that the increase in data breaches is tied to the proliferation of databases containing “tempting troves of customer and financial data” with often outdated and weak security).

3. David W. Opperbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 936 (2016).

4. See George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 WAKE FOREST L. REV. 1, 4 (2016) (“These breaches cause tangible, financial harms to the individual. Identity theft and accompanying fraud constitute a growing type of criminal activity in which a cyber thief impersonates the victim to fraudulently spend the victim’s money.”).

5. Opperbeck, *supra* note 3, at 939.

6. See Katie Bo Williams, *Officials Worried Hackers Will Change Your Data, Not Steal It*, HILL (Sept. 27, 2015), <http://thehill.com/policy/cybersecurity/254977-officials-worried-hackers-will-change-your-data-not-steal-it> [perma.cc/VHJ5-KWPW] (noting that “as security systems get better and hackers are forced to get more creative, manipulation is a likely new cyber vanguard”); Orestis Papakyriakopoulos et al., *Social Media and Microtargeting: Political Data Processing and the Consequences for Germany*, BIG DATA & SOC’Y 1, 2 (2018) (citation omitted) (“[M]icrotargeting presupposes the collection of large amounts of data able to depict the political preferences and other non-political characteristics of voters. . . . Another advantage is that microtargeting allows political actors to target voters from the entire political spectrum, rather than exclusively developing their campaign on the characteristics of the *median voter*, as was the case in the past.”).

7. I have previously argued that current data-breach law should be read broadly and amended as needed. See Ido Kilovaty, *Data Breach Through Social Engineering*, HARV. L. REV. BLOG (Mar. 21, 2018), <https://blog.harvardlawreview.org/data-breach-through-social-engineering> [perma.cc/3LVP-XKTW] (“[W]e should be rethinking our conception of what

explores whether cybersecurity law, in particular data-breach notification law, is able to address these new threats to individual autonomy, privacy, and democracy.

This Article argues that the current threat of online manipulation, as well as other emerging threats online that transcend dated notions of identity theft and financial fraud, require a significant reevaluation, and as a result, an update of the scope and concept of cybersecurity law. This Article calls for an expansion of the meaning of cybersecurity law to include not only data breaches that present some actual risk of identity theft or fraud, but also data breaches that breach *autonomy* and *democracy*.⁸ This Article defines cybersecurity law as the statutes that focus on data security, data-breach notification, post-breach litigation based on common law and statutory claims, computer hacking laws, and laws on information sharing.⁹ Today's data breaches call for a reconceptualization of the law, informed by the concept of information fiduciaries, which among other things, requires that Internet actors secure user information.¹⁰ While this law is largely a decentralized patchwork, the

constitutes a data breach, and subsequently, what sort of activities we wish to delegitimize through our legal system. The statutes can and should be read broadly to include socially engineered breaches; where the law is not sufficiently clear about this, it should be amended. Once we acknowledge that a data breach could take place in the form of manipulation, we could provide better protection for user privacy and security. This would in turn incentivize tech companies to monitor third-parties with whom they share user personal data, and make it harder for malicious actors to take hold of that data.”); *see also* Patricia Hurtado, *Schneiderman Says New York Data Law ‘Outdated and Toothless’*, BLOOMBERG (Mar. 29, 2018), <https://www.bloomberg.com/news/articles/2018-03-29/schneiderman-says-new-york-data-law-outdated-and-toothless> [perma.cc/KTU9-PKPD] (reporting that New York Attorney General Eric Schneiderman announced that he would introduce legislation that would require online service providers to notify “consumers when they learn that users’ personal information was misused”).

8. For an argument on how the current data economy enables democracy to be “hacked,” see Hugo Zylberberg, *Democracy, Hacked: A Security Argument for Data Protection*, LAWFARE (Jan. 26, 2017), <https://www.lawfareblog.com/democracy-hacked-security-argument-data-protection> [perma.cc/82HG-RB3K] (“[T]he business model of the Newsfeed rests on the profit generated by this ‘targeting-and-convincing’ infrastructure. First, companies like Facebook or Twitter collect personal data on their users to profile them (the targeting phase). Second, these segments of users are served ads that are paid for by third parties (the convincing phase). If the ad content shifts from commercial to political, Facebook and Twitter’s Newsfeed algorithms can thereby be co-opted into a ‘micro-propaganda machine.’ This machine, during election cycles, can then be exploited not just by companies but also for the political purposes of either national or foreign organizations. Indeed, the massive collection of personal data has enabled political entrepreneurs, both at home and abroad, to hack democracy.”).

9. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1011 (2018) (listing the statutes that would fall under the definition of U.S. data security statutes).

10. The concept of information fiduciaries could apply in cases of autonomy breaches. As Jack Balkin suggests in a blog post on the political economy of freedom of speech,

regulatory model behind it is primarily focused on financial harms.

A. CYBERSECURITY & DATA-BREACH NOTIFICATION LAW

Cybersecurity law itself is a fairly broad concept. It involves a patchwork of federal and state statutes and regulations—an “uncoordinated mishmash” of sorts.¹¹ Cybersecurity law is not fully capable of protecting the three basic aspects of information security: confidentiality, integrity, and availability.¹² Data-breach notification law, the focus of this Article, represents certain tradeoffs, balances, and priorities set by cybersecurity law. It reflects the goals that cybersecurity law sets for itself—primarily protection from and mitigation of identity theft and financial fraud. Data-breach notification law deals with a very concrete aspect of cybersecurity—post-breach notification. Though notification presupposes that a data breach has occurred and that the breached entity is under an obligation to notify its consumers, both requirements are the basic building blocks of data-breach notification law.¹³ Data-breach notification laws represent the broader inability of cybersecurity law to adapt to new threats presented by the abuse of personal and nonpersonal information. The consideration of data-breach notification law as the first step in responding to manipulation may facilitate the development of other cybersecurity statutes. The inclusion of manipulation within the scope of incidents covered by data-breach notification law can further develop and

if you want a simple example of what difference the concept of information fiduciaries would make, take a look at the recent Facebook/Cambridge Analytica scandal. It’s important to focus not only on the particular example of Facebook’s negligence in dealing with Aleksandr Kogan and Cambridge Analytica, but also on the ensuing revelations: Facebook’s practices were merely the tip of a far larger iceberg—a series of unwise decisions through which Facebook allowed its business partners to access its end-users’ social graphs. In my view, Facebook probably violated all three duties of care, confidentiality and loyalty. Facebook did not take sufficient care to vet its business partners, it breached its duties of confidentiality toward its end users, and it allowed its end-users to be manipulated by its business partners.

Jack M. Balkin, *The Political Economy of Freedom of Speech in the Second Gilded Age*, LAW & POL. ECON. (July 4, 2018), <https://lpeblog.org/2018/07/04/the-political-economy-of-freedom-of-speech-in-the-second-gilded-age> [perma.cc/8CHG-EMH6].

11. Kosseff, *supra* note 9, at 988.

12. See CHARLES P. PFLEEGER ET AL., SECURITY IN COMPUTING 7 (5th ed. 2015).

13. CAL. CIV. CODE § 1798.82 (West 2019) (requiring data breach notification invocation once a: (1) “breach of the security of the system” occurs and; (2) the breached entity determines that there aren’t any factors precluding notice to consumers). These factors vary by state and may include an ongoing law enforcement investigation or a determination that there is no risk of harm to consumers.

inform other cybersecurity statutes on what ought to be protected.¹⁴ This expansion is part of a larger trend associated with cybersecurity law—its two dominant regulatory models, information sharing and deterrence.¹⁵

While data-breach notification law has played an important, albeit imperfect,¹⁶ role in addressing the more traditional form of data breaches, it has failed to address risks other than identity theft or financial fraud.¹⁷ For example, there is a risk that breached information will be used for online manipulation and microtargeting as a direct result of a data breach. Although many concerns exist in today's data-breach landscape, this Article focuses on online manipulation through psychographic profiling to demonstrate the advanced threats presented by data breaches.¹⁸ The failure to contain the effects of online manipulation is attributed not to the law or to its structure alone. Actually, the law on data breach notification has some plasticity that would allow it to apply to new cybersecurity threats in the same manner that it currently applies to identity theft and fraud. The problem, rather, is how the law is being perceived, applied, adjudicated, and used in different contexts. It is a question of the foundations of cybersecurity law, whether these foundations work today, and whether we should reevaluate what they ought to be.

B. BIG DATA & MANIPULATION

A lot can be said about how emerging technological advances bolstered the ability to analyze and use data in new and sophisticated ways.¹⁹ While data

14. See Jeff Koseff, *Cybersecurity of the Person*, 17 FIRST AMEND. L. REV. 343, 345 (2018) (arguing that cybersecurity law is narrowly focused on financial fraud and identity theft but should also apply to new harms that include “non-economic harms, such as online harassment, cyberbullying, and revenge pornography”).

15. Andrea Matwyshyn, *Cyber!*, 2017 BYU L. REV. 1109, 1126–27 (2018).

16. Some scholars refer to this imperfection as “data breach fatigue.” See Mathew Ingram, *Are We All Suffering From Data Breach Fatigue?*, COLUM. JOURNALISM REV. (Oct. 3, 2018), https://www.cjr.org/the_media_today/facebook-data-breach.php [perma.cc/HJ8N-WT7Y].

17. Koseff, *supra* note 9, at 358 (“What do data breach notification laws not cover? For starters, they do not require individuals to be notified of the disclosure of information that could be used to stalk, harass, or dox them.”).

18. See, e.g., Daniel Castro, *It Would Have Taken More Than Privacy Laws to Prevent the Cambridge Analytica Scandal*, HILL (Apr. 10, 2018), <http://thehill.com/opinion/technology/382443-it-would-have-taken-more-than-privacy-laws-to-prevent-the-cambridge> [https://perma.cc/Z92Y-G6SL] (arguing that privacy laws have failed in protecting user data from Cambridge Analytica, thus claiming that the private sector should find solutions to the problem of online manipulation in the future, rather than legislators).

19. See Louise Amoore & Volha Piotukh, *Life Beyond Big Data: Governing with Little Analytics*, 44 ECON. & SOC'Y 341, 344 (2015) (“[O]ne of the many problems with a pervasive focus on ‘big’ and ‘data’ is that the finite and granular minutiae of the analytics are

has always had its face value—derived from its representation of certain information about something or someone—its value nowadays also originates from the ability to make sense of it on a higher level, a secondary use of sorts enabling software to explain patterns and inferences based on thousands of variables.²⁰ This secondary use provides a deeper insight into the data subject’s personality, weaknesses, vulnerabilities, and more.

This “big data” is becoming increasingly valuable due to what machine learning algorithms can do with it. Primarily, big data may reveal patterns, abnormalities, and trends that are not visible to the naked human eye. Its capability and success rate in doing so are also gradually increasing based on user feedback and outcomes, making inferences informed by psychology, sociology, and behavioral economics.²¹ On a more individual level, highly detailed and nuanced data about someone, paired with advanced technology and insights from online behaviorism, allows for malicious actors to more effectively manipulate the individual by exploiting existing biases and vulnerabilities.²² While manipulation has existed throughout human history as part of human interaction,²³ today, manipulation proliferates on the Internet,

overlooked.”). However, certain commentators cast doubt on the assertion that big data has some exceptional power or utility for the purpose of prediction of behaviorism. *See, e.g.*, Caryn Devins et al., *The Law and Big Data*, 27 CORNELL J.L. & PUB. POL’Y 357, 371–72 (2017) (“Big Data’s supposed objectivity and predictive power are overstated, at least when applied to highly complex evolutionary systems such as the legal system. Data always require interpretation, which necessitates theory and, correspondingly, evaluative judgment by humans. Further, Big Data cannot foresee the fundamentally creative, non-algorithmic evolution of the legal system, and its predictive power is limited.”).

20. *See* Sofia Grafanaki, *Autonomy Challenges in the Age of Big Data*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 803, 805 (2017) (describing the future of algorithmic regulation, “where decisions about individuals and society in general are made by software taking into account thousands of variables not interpretable in human language”).

21. *See* Karen Yeung, *‘Hypernudge’: Big Data as a Mode of Regulation by Design*, 20 INFO., COMM. & SOC’Y 118, 119 (2017) (“[T]he technology and the process comprise a methodological technique that utilises analytical software to identify patterns and correlations through the use of machine learning algorithms applied to (often unstructured) data items contained in multiple data sets, converting these data flows into a particular, highly data-intensive form of knowledge.”).

22. *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014) (identifying the role of behavioral economics in manipulating consumers: “[t]he interplay between rational choice and consumer bias that is at the heart of behavioral economics helps illustrate how information and design advantages might translate into systematic consumer vulnerability”).

23. *See* Marcello Ienca & Effy Vayena, *Cambridge Analytica and Online Manipulation*, SCI. AM. (Mar. 30, 2018), <https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation> [perma.cc/7JBG-MTFK] (“Attempts to manipulate other people’s unconscious mind and associated behavior are as old as human history. In Ancient Greece, Plato warned against demagogues: political leaders who build consensus by appealing

media, politics, markets, family, friendships, relationships, and life.²⁴

But recent technological advancements, the availability of data, and the global nature of the Internet give manipulation a far more menacing form, especially as manipulation becomes pervasive in U.S. political processes and culture.²⁵ As some commentators put it—“[s]ince we are never totally free of outside influence, what gives us (part) authorship over our own actions is that we regard our own reasons for acting as authoritative. Manipulation thwarts that.”²⁶

C. INFORMATION FIDUCIARIES

The enormous scope of adverse effects and emerging information practices brought about by new technologies requires government regulation that would mitigate the harms anticipated from their use or requires that the industry self-regulate by enacting precautionary measures to decrease the likelihood that such harms would materialize.²⁷

For example, Jack Balkin’s *Information Fiduciaries in the Digital Age* argues that we create a fiduciary obligation upon Internet platforms when we entrust them with our information assets in order to keep our information confidential and secure.²⁸ Online service providers would assume these duties because they

to popular desires and prejudices instead of rational deliberation. However, the only tool demagogues ancient Athens could use to bypass rational deliberation was the art of persuasion. In today’s digital ecosystem, wannabe demagogues can use big data analytics to uncover cognitive vulnerabilities from large user datasets and effectively exploit them in a manner that bypasses individual rational control.”).

24. See Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MARKETING BEHAV. 213, 218 (2015).

25. Roberto J. González, *Hacking the Citizenry? Personality Profiling, ‘Big Data’ and the Election of Donald Trump*, 33 ANTHROPOLOGY TODAY 9, 11 (2017) (explaining how personality profiling software and tools have been used since Obama’s 2012 presidential campaign).

26. Helen Nissenbaum et al., *Online Manipulation: Hidden Influences in a Digital World* 16 (Jan. 8, 2019) (unpublished manuscript) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006 [<https://perma.cc/4KJU-DABA>].

27. See, e.g., *What is App Review For Facebook Login*, FACEBOOK <https://developers.facebook.com/docs/facebook-login/review/what-is-login-review> [perma.cc/UG8H-T87J] (last visited Aug. 13, 2019) (describing a process developed by Facebook following the Cambridge Analytica scandal to ensure that developers are transparent and accountable to their uses of Facebook user data). For a critical view of self-regulation in the manipulation context, see Terrell McSweeney, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is The FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 514 (2018), in which McSweeney notes that the phenomena of online manipulation and influence “underscore the power of increasingly sophisticated predictive technology and the limitations of the United States’ largely self-regulatory approach to consumer data rights, privacy, and security.”

28. See generally Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

act as information fiduciaries.²⁹ As information fiduciaries, a person or business dealing with sensitive information should “have duties of care, confidentiality, and loyalty toward the people whose data they collect, store, and use.”³⁰

While the importance of the imposition of these duties cannot be overstated, serious limitations exist to imposing such duties directly on online service providers when it comes to online manipulation. The fiduciary approach assumes business-as-usual and does not consider the proliferation of data breaches that compromise the same information held by these information fiduciaries. These data breaches may trigger information fiduciaries’ duty of loyalty to their customers.³¹ Failing to protect that information, and perhaps even the collection of certain information, may breach that duty. Similarly, failing to notify regulators or consumers that a breach has occurred ought to violate that duty. In the context of data breach, the duty of loyalty would require additional steps that would guide companies on how to notify their consumers and approach the issue. While holding online service providers as information fiduciaries may mitigate some of the risks associated with data compromise, it does not fully capture data that does not seem “sensitive” or relationships between customers and entities that are not deemed fiduciaries.

Expanding data-breach notification law is not only a response to the information fiduciaries approach, but also a legal intervention (in particular, through tort law) to the mere enablement of online manipulation by these fiduciaries.³² After all, the failure to secure personal information may create

29. See Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/> [perma.cc/Y46P-PPJW] (“An *information fiduciary* is a person or business that deals not in money but in information. Doctors, lawyers, and accountants are examples; they have to keep our secrets and they can’t use the information they collect about us against our interests. Because doctors, lawyers, and accountants know so much about us, and because we have to depend on them, the law requires them to act in good faith—on pain of loss of their license to practice, and a lawsuit by their clients. The law even protects them to various degrees from being compelled to release the private information they have learned.”).

30. Balkin, *supra* note 10.

31. In general, an information fiduciary is an extension of the general fiduciary duty in law. See Balkin & Zittrain, *supra* note 29 (“In the law, a *fiduciary* is a person or business with an obligation to act in a trustworthy manner in the interest of another. Examples are professionals and managers who handle our money or our estates. An information fiduciary is a person or business that deals not in money but in information.”).

32. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1558 (2005) (exploring the idea that certain software vulnerabilities and defects enable cybercrime and therefore should be considered a tort: “[t]he software industry has simply abdicated to third parties its responsibility for limiting high-risk

new threats against the data subjects who lose their information. As online service providers collect ever-increasing amounts and categories of data about us, regardless of whether this data was given voluntarily or involuntarily,³³ malicious actors are increasingly empowered by the availability of such data troves for the purpose of manipulation.³⁴ Intervening through data-breach notification law could therefore resolve some of the difficulties with third-party misuse of personal information, since these parties are rarely in direct contractual relationships with the manipulated victims.³⁵ This would effectively shift the disclosure and mitigation burden back to the breached entity.

Current data-breach notification law could potentially mitigate online manipulation, but current data-breach jurisprudence emphasizes a strict tangibility approach. Under this framework, the legitimacy of a claim for harm caused by a data breach hinges upon the actual, *tangible* harm sustained by the victims, not whether an *intangible* harm took place or risk of such harm increased.³⁶

design defects. “The problem is that those responsible for securing our personal data are rarely the ones who pay the cost of securing it and in many cases are not the same people with whom we have entrusted our data in the first place’”) (citation omitted).

33. See Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1411 (2001). It is understood that online service providers obtain personal data about us in two ways—“(1) by directly collecting information from users (registration and transactional data); and (2) by surreptitiously tracking the way people navigate through the Internet (clickstream data).” *Id.*

34. See Alexis Madrigal, *What Took Facebook So Long?*, ATLANTIC (Mar. 18, 2018), <https://www.theatlantic.com/technology/archive/2018/03/facebook-cambridge-analytica/555866> [perma.cc/KQ8H-RE4P] (“If one were to systematically crawl through all the data that could be gleaned from just a user’s basic information, one could build a decent picture of that person’s social world, including a substantial amount of information about their friends.”).

35. See McSweeney, *supra* note 27, at 517–18 (“However, this framework [FTC enforcement] does not address the use of personal information by third parties and data brokers who have no direct consumer-facing relationship, nor does it adequately reach unanticipated uses of data as inputs for complex algorithms or by the increasingly powerful platforms that mediate most consumers’ Internet experience.”).

36. See, e.g., *Bradix v. Advance Stores Co.*, No. 16-4902, 2016 WL 3617717, at *1–4 (E.D. La. July 6, 2016) (dismissing a claim of injury because the misuse by criminals of breached personal information for car financing did not affect the plaintiff’s credit score); *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-MD-2586, 2016 WL 81792, at *8 (D. Minn. Jan. 7, 2016) (dismissing the lawsuit because a single plaintiff’s unauthorized credit card charge does not constitute harm and therefore the plaintiff lacks standing); *Doe v. Chao*, 540 U.S. 614, 625 (2004) (the government sending social security numbers to unauthorized parties [therefore violating the Privacy Act of 1974] does not constitute harm); see also Daniel Solove & Danielle Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 755 (2018) (discussing the absurdity of not recognizing other data-breach harms, such as anxiety and risk: “[r]equiring harm to be visceral and vested has severely restricted the recognition of data-breach harms, which rarely have these qualities. Data-breach harms are not easy to see, at least not in any physical way. They are not tangible like broken limbs and

This outdated approach fails to recognize a neoteric, and perhaps more devastating type of personal information misuse—manipulation—a harm that is different from identity theft or fraud and which transcends the notion of pure economic injury.³⁷ The current focus of data-breach jurisprudence is therefore ineffective and increasingly irrelevant in today’s data analytics reality, requiring a conceptual adaptation and transformation.

What is currently missing from the literature is a comprehensive account of the evolving and necessary role of data-breach notification law and how it could be leveraged to meet the future landscape of data exploitation before regulators create more advanced and direct forms of norms and regulations. This Article addresses this gap.

This Article contributes to the literature by advancing two main arguments. First, the risk of online manipulation resulting from a data breach should be sufficient grounds to trigger data-breach notification law. In other words, the question is whether there was a loss of information that can objectively be used for microtargeting, or any other harm that would not qualify as either identity theft or financial fraud. This would mean that breached companies would have to inform consumers and regulators when there is a risk of manipulation associated with compromised personal information, even if there is no risk of identity theft or fraud. Second, adopting such legal intervention would result in crucial benefits for society and the digital ecosystem—reducing the information asymmetry between consumers and firms, indirectly regulating data collection, increasing information security, remedying manipulation of victims, and strengthening regulatory oversight over data collectors.³⁸ While we may believe that new socio-technological problems require tailored regulatory solutions, and indeed many of them do in the long-term, this is not necessarily the case in the interim, where existing tools may still prove useful

destroyed property. Instead, the harm is intangible. Data breaches increase a person’s risk of identity theft or fraud and cause emotional distress as a result of that risk. Despite the intangible nature of these injuries, data breaches inflict real compensable injuries. Data breaches raise significant public concern and generate legislative activity”); Ashenmacher, *supra* note 4, at 5 (“But have individuals been harmed even where their PII [personally identifiable information] has not been used to commit fraud? . . . By and large, American law has responded with an unsympathetic ‘no.’”); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2279 (2015) (“If people’s data are leaked, but they do not suffer from identity theft, are they harmed? Although courts struggle to recognize harm, there clearly seems to be a substantial negative impact on people’s lives.”).

37. See Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 70 (2003) (“[T]he appropriation tort . . . is aimed at protecting a broader sphere of identity than mere names or physical likenesses and . . . [it] is intended to protect dignitary, rather than economic, interests.”).

38. See *infra* Part IV.

in addressing these challenges.

The Article proceeds as follows. Part I explores the tenets of online manipulation in the context of psychographic profiling and provides an analysis of the perils of manipulation and how manipulation threatens autonomy, democracy, and freedom from experimentation. Part II provides an overview of where current data-breach notification law stands when it comes to data being misused for targeted user manipulation, highlighting some of the gaps that require reevaluation in light of online manipulation practices. Part III explores the ways in which embedding online manipulation within data-breach notification law would benefit society and consumers at large. It considers and builds on existing scholarship on privacy harms, cybersecurity and data-breach litigation, and online manipulation.³⁹ In addition, this Part will also address some of the hurdles requiring further research on how to meet these challenges. Finally, the Article concludes in Part IV by proposing a reconceptualization of data-breach jurisprudence to meet a world of digital manipulation.

II. ONLINE MANIPULATION AND PSYCHOGRAPHIC PROFILING

Manipulation for marketing and other purposes is not a novel phenomenon. In the late 1950s, motivational analysis gave rise to “depth marketing,”⁴⁰ which allowed advertisers to target potential consumers through subliminal advertising, increasing the likelihood that consumers would purchase a product.⁴¹ Scholars first raised concerns over privacy stemming from manipulation in 1971,⁴² and today it draws even more attention from legal academics.⁴³

39. See, e.g., Solove & Citron, *supra* note 36, at 737; Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361 (2014); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2015); Sunstein, *supra* note 24; Tansy Woan, *Searching for an Answer: Can Google Legally Manipulate Search Engine Results?*, 16 U. PENN. J. BUS. L. 294 (2013); Susser et al., *supra* note 23.

40. See generally VANCE PACKARD, *THE HIDDEN PERSUADERS* (1957).

41. Calo, *supra* note 22, at 997.

42. See ARTHUR R. MILLER, *THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS* 442–43 (1971) (predicting risks that threaten the “line between the use of cybernetics to understand an individual and its use to control or affect his conduct . . . [which] is shadowy at best”).

43. Sunstein, *supra* note 24; see generally Eric Posner, *The Law, Economics, and Psychology of Manipulation*, (Coase-Sandor Inst. for Law and Econ., Working Paper No. 726, 2015).

In *Digital Market Manipulation*, Ryan Calo explores the question of manipulation for marketing purposes. Focusing on the new legal and ethical questions that such a phenomenon raises, Calo asks whether at a certain point, these techniques reach a level of severity and misalignment of interests between the manipulator and manipulee that justifies legal intervention.⁴⁴ Calo mentions information-based interventions focused on mandatory disclosure as an example of a legal intervention seeking to minimize, or even negate, the harm of manipulation.⁴⁵ If manipulation subjects are informed, the potency of manipulation may be weakened, though it may not fully disappear.⁴⁶ The same information-based intervention needs to be explored with regard to online manipulation, not solely for marketing, but even more so for political and ideological purposes, e.g., microtargeted political ads that leverage individual vulnerabilities and personality traits.⁴⁷ If a sufficiently sophisticated and motivated entity obtains access to a diverse set of data points about each individual, it would be able to construct manipulatable personality profiles and exploit them. Indeed, Calo considers “how should law or society treat political ads by candidates or causes that leverage individual biases to make their campaigns more effective? Such techniques portend an arguably greater threat to autonomy.”⁴⁸ Calo does not directly answer this question.

Different U.S. presidential campaigns have similarly used “symbolic manipulation by design, playing on deeply held beliefs in the electorate” to improve their chances of success in the election.⁴⁹ Technology makes these efforts much easier, more effective, and potentially more dangerous for protected values like free speech, autonomy, and democracy.⁵⁰ Because

44. Calo, *supra* note 22, at 998.

45. *Id.* at 1013.

46. This intuition dates back to 1914, when Louis Brandeis claimed that “[p]ublicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants” LOUIS BRANDEIS, *What Publicity Can Do, in OTHER PEOPLE’S MONEY AND HOW THE BANKERS USE IT* 92, 92 (1914).

47. See Frederik J. Zuiderveen Borgesius et al., *Online Political Microtargeting: Promises and Threats for Democracy*, 14 *UTRECHT L. REV.* 82, 82 (2018) (“Through political microtargeting, a political party can identify the individual voters which it is most likely to convince. Additionally, a party can match its message to the specific interests and vulnerabilities of these voters. Modern online marketing techniques promise to make microtargeting even more tailored to individual voters, and more effective.”).

48. Calo, *supra* note 22, at 1049.

49. J.R. McLeod, *The Sociodrama of Presidential Politics: Rhetoric, Ritual, and Power in The Era Of Teledemocracy*, 101 *AM. ANTHROPOLOGIST* 359, 360 (1999).

50. See Zeynep Tufekci, *Facebook and Engineering the Public*, *MEDIUM* (June 29, 2014), <https://medium.com/message/engineering-the-public-289c91390225> [perma.cc/TV56-NYLM] (“[T]hese large corporations (and governments and political campaigns) now have new tools and *stealth* methods to quietly model our personality, our vulnerabilities, identify our networks, and effectively nudge and shape our ideas, desires and dreams. These tools are new,

politicians can continue to capitalize on the perceived political advantages without being held accountable for the many dangers, these manipulation efforts will likely persist in the political context.⁵¹ This is not the sole reason why legal intervention is now needed, but it exacerbates the privacy and autonomy challenges arising from online manipulation.

Online manipulation may sound like an overly broad concept, with some parts of it justifying legal intervention while others do not.⁵² It could vary in degree, intrusiveness, sophistication, motives, purpose, actors, and tools.⁵³ As Daniel Susser, Beate Roessler, and Helen Nissenbaum point out in their work *Online Manipulation*,⁵⁴ manipulation could take the form of a nudge, persuasion, deception, coercion, and more.⁵⁵ As Cass Sunstein puts it in *Fifty Shades of Manipulation*—“it has at least 50 shades.”⁵⁶ Some of these shades are socially and legally acceptable, while others are not.⁵⁷ For example, persuasion is seen as a normal rhetorical tool, where “people are given facts and reasons, presented in a sufficiently fair and neutral way.”⁵⁸ However, this would not be the case for severe coercion, where facts and reasons are not presented to people, but rather these people are forced into a choice they would otherwise not make.⁵⁹

Given this divergent normativity, legal intervention will only be justified for some forms of manipulation and not for others. However, even when justified, it could be shaped in different ways—through direct regulation of the relevant industry (social media, political entities, data brokers, etc.), the data-subjects, or the incentives and disincentives that usually surround this

this power is new and evolving.”).

51. See Nina Burleigh, *How Big Data Mines Personal Info to Craft Fake News and Manipulate Voters*, NEWSWEEK (June 8, 2017), <http://www.newsweek.com/2017/06/16/big-data-mines-personal-info-manipulate-voters-623131.html> [perma.cc/YRF5-D7J2] (“By 2020, behavioral science, advanced algorithms and AI applied to ever more individualized data will enable politicians to sell themselves with ever more subtle and precise pitches.”).

52. See Nissenbaum et al., *supra* note 26.

53. *Id.*

54. *Id.*

55. *Id.*

56. Sunstein, *supra* note 24, at 216.

57. See Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1150 (2011) (arguing, for example, that coercion exists on a spectrum, which determines its permissibility: “[m]any important activities, from air travel to medical care, are premised upon giving up information or revealing one’s body in potentially demeaning and uncomfortable ways. There may indeed be little alternative to surveillance in daily life”).

58. Sunstein, *supra* note 24, at 216.

59. See *id.* at 220; see also JOSEPH RAZ, *THE MORALITY OF FREEDOM* 377 (1988) (contrasting coercion from manipulation by providing that “[m]anipulation, unlike coercion, does not interfere with a person’s options. Instead it perverts the way that person reaches decisions, forms preferences or adopts goals”).

manipulation phenomenon. Manipulations should warrant certain legal intervention in such cases where personal and nonpersonal information can be used in ways that are likely to affect a person's thoughts, opinions, and actions. This Article will use the definition of manipulation developed by Nissenbaum et al.—“imposing a hidden influence on someone by targeting and exploiting their weaknesses or vulnerabilities.”⁶⁰

There are three fundamental components in this definition. First, the manipulation is hidden from the subject, known to the manipulator, and known or unknown to different degrees to others.⁶¹ Data-breach notification law seeks to address exactly this information gap by exposing the existence of a breach and ensuring that potential victims take extra precautions.⁶² Second, the manipulation exploits weaknesses and vulnerabilities of the subject based on data available about her. Manipulators learn these weaknesses and vulnerabilities by using advanced algorithms to analyze thousands of different data points and create a certain personality profile.⁶³ And, third, the manipulation must be targeted, meaning that the subject gets served with a certain communication tailored precisely to gain access to the attention, interest, and hopefully action of that individual, whether cognitive or behavioral. While manipulation can be achieved through a variety of techniques, manipulation becomes particularly alarming with the emerging technique of psychographic profiling.⁶⁴

60. Nissenbaum et al., *supra* note 26, at 22.

61. See Nissenbaum et al., *supra* note 26, at 16 (“The hiddenness of manipulative influences explains how it is possible to alienate someone from their own decision-making powers.”).

62. See Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POLY ANALYSIS & MGMT. 256, 262 (2011) (“Consumer precaution should increase after the passage of the law because, as more consumers are notified of a breach involving their sensitive information, they may take steps to reduce the risk and the costs of becoming a victim of identity theft. For example, they could notify their financial institutions to block transactions and cancel accounts or apply credit freezes and fraud alerts. Moreover, such notices also could serve to increase consumer awareness in general, making them alert to possible identity thefts. Therefore, a primary effect of data breach disclosure laws should be the reduction of the incident of identity theft, as well as a mitigation of its impact, via better consumer precaution.”).

63. See Katy Steinmetz, *The Facebook Data Cambridge Analytica Took Was Either Extremely Valuable or Totally Worthless*, TIME (Mar. 22, 2018), <http://time.com/5207764/cambridge-analytica-facebook-data> [perma.cc/T42W-M7LB] (“The trove included information like people’s names, locations, genders and things users have “liked” on Facebook, which a company whistleblower said it planned to use to exploit “the mental vulnerabilities of people” with targeted political messages . . . the firm’s [Cambridge Analytica] intention [was] to use “likes” to help build algorithms that can predict the personality traits of voters.”).

64. See *infra* Section II.A.

To be clear, data-breach notification law is but one solution to a broader cybersecurity law problem, and online manipulation is an emerging threat that cybersecurity law should be concerned with, but it is one harm out of many. Jeff Kosseff, for example, argues that cybersecurity law is overly reliant on financial harm, whereas there is a myriad of other online harms that cybersecurity law should adapt to, such as risk, anxiety,⁶⁵ revenge pornography, and online harassment.⁶⁶ Psychographic profiling is a case study which highlights the emerging cybersecurity harms that law should respond to.

A. PSYCHOGRAPHIC PROFILING AS MANIPULATION

Psychographic profiling (or psychographics) is a technique that creates a personality profile of an individual based on five main personality traits. Social psychologists have long recognized the ability to profile individuals based on the “Big Five” personality traits: openness, conscientiousness, extroversion, agreeableness, and neuroticism.⁶⁷ Initially, psychographic profiling was ineffective due to data collection problems. However, data collection problems have been resolved due to the wide availability of data.⁶⁸ Psychographic profiling does not necessarily have to be nefarious. For example, it could be used to motivate people to engage in healthier activities and habits,⁶⁹ as well as make consumers more comfortable and their experiences more convenient. However, to date, these targeting methods hold the most potential when it comes to influencing and manipulating individuals.⁷⁰

In 1999, entrepreneur Thomas Gerace created a patent that provided an early example of how computer systems could incorporate psychographic profiling. Gerace created a computer program that determined the

65. See generally Solove & Citron, *supra* note 36.

66. See generally Kosseff, *supra* note 11, at 355.

67. González, *supra* note 25, at 10.

68. See generally Ali Fenwick, *Psychographics: How Big Data is Watching You*, HULT BLOG (2018), <https://www.hult.edu/blog/psychographics-big-data-watching/> [<https://perma.cc/9TEM-TSC7>].

69. See generally Sarah Hardcastle & Martin Hagger, *Psychographic Profiling for Effective Health Behavior Change Interventions*, 6 FRONTIERS PSYCHOL., Jan. 2016, at 1, 1–2 (“Research has identified multiple correlates of health behavior change, and interventions have been developed to target these factors. Such interventions have shown significant effects in changing behavior” though, researchers believe that a more individualized form of intervention may be required to be more effective overall.”).

70. See generally *id.*; Kalev Leetaru, *Data Breaches, Psychological Profiling, Voter Modeling: Inside the Big Data World of Campaign 2016*, FORBES (Jan. 1, 2016), <https://www.forbes.com/sites/kalevleetaru/2016/01/01/data-breaches-psychological-profiling-voter-modeling-inside-the-big-data-world-of-campaign-2016/#4ffc8def7c4f> [perma.cc/6CMY-EBHH] (“This is the future of political campaigning in the 21st century in which we are all just data points in giant psychographic models that attempt to figure out how best to make us vote a certain way.”).

psychographic profile of a user based on her “history and/or pattern of user activity which in turn [was] interpreted as a user’s habits and/or preferences.”⁷¹ This sort of dataset is explicitly distinguished from demographics, where only personal details such as gender, age, income bracket, and occupation are taken into account.⁷² This distinction, even tension, between demographics and psychographics is crucial to realizing that a reform of data-breach notification law is desperately needed, since data-breach law is for the most part concerned with demographic information. This will be discussed further in Part IV of this Article.

Manipulation by itself is not an absolute evil. Rather, it depends on whether there is an alignment of interests between the subject and the manipulator, both on the individual and collective levels.⁷³ As Calo aptly suggests, legal intervention would be justified whenever there is a divergence between these interests, leading to one side leveraging this gap in information to her own benefit.⁷⁴ This is where the regulator should intervene.

Recently, the British political consultancy firm, Cambridge Analytica, used psychographic profiling to conduct political manipulation, allegedly influencing the outcomes of the 2016 U.K. referendum to withdraw from the European Union,⁷⁵ and the 2016 U.S. presidential election.⁷⁶

Cambridge Analytica, a counterpart of the data mining and analysis firm SCL Group, has become infamous for improperly accessing the sensitive and personal information of 87 million Facebook users in an unauthorized manner.⁷⁷ This personal information was obtained through data collected by a “test your personality” research application (app) developed by a University of Cambridge neuroscience lecturer, Aleksandr Kogan, using the Facebook application programming interface (API).⁷⁸ The data collected by this app was

71. U.S. Patent No. 5,991,735 (issued Nov. 23, 1999).

72. *Id.*

73. *See* Calo, *supra* note 22, at 1023.

74. *Id.*

75. *See generally* Carole Cadwalladr, *The Great British Brexit Robbery: How Our Democracy Was Hijacked*, *GUARDIAN* (May 7, 2017), <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> [perma.cc/24RV-LT2R] (“Cambridge Analytica . . . the data analytics firm that played a role in both Trump and Brexit campaigns.”).

76. González, *supra* note 25, at 9.

77. *See* Issie Lapowsky, *Facebook Exposed 87 Million Users to Cambridge Analytica*, *WIRED* (Apr. 4, 2018), <https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica> [perma.cc/HJL8-BNRN].

78. Ethan Zuckerman, *This Is So Much Bigger Than Facebook*, *ATLANTIC* (Mar. 23, 2018), <https://www.theatlantic.com/technology/archive/2018/03/data-misuse-bigger-than-facebook/556310> [perma.cc/EL2X-7CGA] (“Aleksandr Kogan, the Cambridge University researcher who built a quiz to collect data on tens of millions of people, didn’t break into

then passed on to Cambridge Analytica, in what some would assert to be a clear breach of research ethics.⁷⁹

Cambridge Analytica, hired by the Leave.EU campaign⁸⁰ as well as Donald Trump's⁸¹ and Ted Cruz's⁸² presidential campaigns, offered these campaigns the data obtained from the app, and more importantly—the analytics based on that data. For example, when working for the Cruz campaign, Alexander Nix, then CEO of Cambridge Analytica, explained that the consultancy firm focused on 45,000 likely Iowa Republicans participating in the caucus who needed a little “persuasion message” to vote for Cruz.⁸³ Cambridge Analytica's psychographic profiling technique managed to craft targeted messages to voters based on “close to 4- or 5,000 data points on every adult in the United States.”⁸⁴ Cambridge Analytica's use of data for effective manipulation through psychographic profiling reflects the striking breadth of data points and their analytical potential, which are part of a “data rich society, in which specific entities have the ability to collect and utilize an immense amount of data about a single individual.”⁸⁵ This technique of manipulation has rightfully earned these techniques labels such as “mind-reading software” and “weaponized AI propaganda machine,” which swayed voting preferences in many of its “persuadable” targets.⁸⁶ These methods were largely reconstructed based on tools developed by psychologist Michal Kosinski, who argued that digital records of an individual can reveal his or her personality traits to a high degree.⁸⁷

Facebook's servers and steal data. He used the Facebook Graph API, which until April 2015 allowed people to build apps that harvested data both from people who chose to use the app, and from their Facebook friends.”)

79. *See id.*

80. Carole Cadwalladr & Mark Townsend, *Revealed: The Ties That Bound Vote Leave's Data Firm to Controversial Cambridge Analytica*, GUARDIAN (Mar. 24, 2018), <https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions> [perma.cc/A9VM-PJ42].

81. Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> [perma.cc/LEL3-P3P5].

82. Harry Davies, *Ted Cruz Using Firm That Harvested Data on Millions of Unwitting Facebook Users*, GUARDIAN (Dec. 11, 2015), <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> [perma.cc/6TEL-S3GY].

83. Nina Burleigh, *How Big Data Mines Personal Info to Craft Fake News and Manipulate Voters*, NEWSWEEK (June 8, 2017), <http://www.newsweek.com/2017/06/16/big-data-mines-personal-info-manipulate-voters-623131.html> [perma.cc/98JL-PKRB].

84. *Id.*

85. Tal Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES IN LAW 157, 169 (2019).

86. González, *supra* note 25, at 9.

87. *Id.* at 10.

Kosinski created a search engine for specific profiles—“all anxious fathers . . . all angry introverts . . . all undecided Democrats.”⁸⁸ This enabled Cambridge Analytica to classify individuals within thirty-two distinct personality types—as well as slice and dice even further within these personality types—for the purpose of political microtargeting.⁸⁹ While some commentators are skeptical as to whether Cambridge Analytica was even remotely successful in its goal,⁹⁰ it is likely that the data harvested by Cambridge Analytica was used as a “training set” for future manipulation operations, which could prove successful.⁹¹ A potential failure of today’s manipulation efforts does not necessarily negate the threat indefinitely.

The intuition amongst many who have learned about Cambridge Analytica’s dealings is that such manipulation is wrongful, as it unduly infringes on autonomy, democracy, and freedom from experimentation. But should manipulation be *legally* wrongful?⁹² It is critical to understand what makes this phenomenon so wrongful that legal intervention is required.

B. THE WRONGFULNESS OF ONLINE MANIPULATION

What makes online manipulation so exceptional that it requires legal intervention? This Article makes three main arguments to support the claim that manipulation is wrong and therefore requires legal intervention. Although these arguments are most often discussed in the context of advertising and marketing, they are nonetheless applicable to the political context as well.

88. *Id.* (citing Hannes Grassegger & Mikael Krogerus, *The Data That Turned The World Upside Down*, MOTHERBOARD (Jan. 28, 2017), https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win [perma.cc/R9QL-PQ2U]).

89. JEFFREY C. SHUMAN ET AL., COLLABORATIVE COMMUNITIES: PARTNERING FOR PROFIT IN THE NETWORKED ECONOMY 68 (2001) (discussing potential developments in profiling tools that “slice and dice the reams of clickstream data Web sites collect into even finer descriptions of consumer profiles”).

90. *See generally* Antonio Garcia Martinez, *The Noisy Fallacies of Psychographic Targeting*, WIRED (Mar. 19, 2018), <https://www.wired.com/story/the-noisy-fallacies-of-psychographic-targeting> [https://perma.cc/B23D-HGZ4] (“[I]f this psychographics business is so effective, why isn’t it commonly used by smart e-commerce players like Amazon, or anyone else beyond the brand advertisers who like keeping old marketing folklore alive?”).

91. *See* Alexis Madrigal, *What Took Facebook So Long?*, ATLANTIC (Mar. 18, 2018), <https://www.theatlantic.com/technology/archive/2018/03/facebook-cambridge-analytica/555866> [https://perma.cc/4JWE-K6Z9].

92. *See generally* Andrew Keane Woods, *The Cambridge Analytica-Facebook Debacle: A Legal Primer*, LAWFARE (Mar. 20, 2018), <https://www.lawfareblog.com/cambridge-analytica-facebook-debacle-legal-primer> [perma.cc/QH95-7KMF] (discussing legal issues arising from Cambridge Analytica).

These arguments focus on autonomy,⁹³ democracy,⁹⁴ and experimentation.⁹⁵

1. *Autonomy*

Online manipulation, if executed properly and successfully, is wrongful because it impairs the ability of individuals to make independent and informed opinions and decisions.⁹⁶ Manipulation infringes on individual autonomy because personal information is exposed to unauthorized entities and used to target the freedom of choice. It effectively deprives individuals of their agency⁹⁷ by distorting and perverting the way in which individuals typically make decisions.⁹⁸ This should be contrasted with rational persuasion, which is contrary to what manipulation stands for.⁹⁹

Julie Cohen acknowledges that meaningful autonomy can be achieved through the adoption of robust information privacy laws and the protection of information relating to individuals and their personalities.¹⁰⁰ In her dynamic theory of information privacy, Cohen explains that in a no-privacy reality, surveilling individuals “will constrain, ex ante, the acceptable spectrum of belief and behavior.”¹⁰¹ However, manipulation affects far more directly the acceptable spectrum of belief and behavior. Therefore, manipulation violates autonomy not only through mere surveillance, but also through acting upon the data surveilled and against the data subject. While Cohen’s work is concerned primarily with privacy, her conclusions on autonomy are equally applicable to emerging cybersecurity threats stemming from manipulation. Privacy and security are typically distinct when it comes to legal regulation, but

93. See Ashenmacher, *supra* note 4, at 8–31 (analyzing autonomy in the context of data-breach harms).

94. The literature originally focused on market manipulation, though in the political context, I would argue that it becomes a democracy concern, since democracy is the “market” equivalent in this context. See, e.g., Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 N.Y.U. L. REV. 630 (1999).

95. See Zarsky, *supra* note 83, at 175 (“Yet a third way to articulate the manipulation-based argument is to note that such actions are unacceptable as they amount to human experimentation.”).

96. Grafanaki, *supra* note 20, at 825 (explaining how predictive algorithms learn from past behavior of the subject, influencing his or her decisions in the future).

97. Sunstein, *supra* note 24, at 226.

98. Charles Mendez, *Deflating Autonomy*, 66 S.C. L. REV. 401, 413 (2014).

99. *The Ethics of Manipulation*, STAN. ENCYCLOPEDIA PHIL. (Mar. 30, 2018), <https://plato.stanford.edu/entries/ethics-manipulation> [perma.cc/3U67-WK8M] (“[I]t seems reasonable to think that because manipulation differs from rational persuasion, it must influence behavior by means that do not engage the target’s rational capacities.”).

100. See Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423 (2000).

101. *Id.* at 1426.

the manipulation threat concerns both privacy and security.¹⁰²

Online manipulation not only constrains beliefs and behaviors *ex ante*, but it creates behavior in the manipulated subjects that would not necessarily take place had they not been manipulated, effectively depriving them of free and unimpaired choices. An act manipulates people if “it does not sufficiently engage or appeal to their capacity for reflection and deliberation.”¹⁰³ A deontological objection suggests that manipulation negatively affects the ability “to assess, to weigh, to judge” at the actor’s convenience and terms, without consenting to such influence.¹⁰⁴ However, this claim rests on the wrongfulness of the act of manipulation, rather than considering whether the manipulation was successful.

While autonomy is an individual-level concern, manipulation could also be wrongful because of its collective impact on democracy. Assuming an individual is successfully manipulated, the individual-level harm is negligible in the political sphere—say, one vote in favor of candidate A, instead of candidate B, out of millions of other voters. However, collectively, if a sufficiently large group of individuals is targeted by online manipulation, the results can be significant.¹⁰⁵ In that case, candidate A would gain a substantial advantage over candidate B, potentially impacting the electoral results.

Political processes throughout the world can be manipulated through social media in way that impairs voter’s ability to autonomously reflect and rationalize individual choices. For example, the Russian interference in the 2016 U.S. presidential election and the U.K. referendum on the secession from the European Union (Brexit)¹⁰⁶ through social media herald the future of

102. See Matwyshyn, *supra* note 15, at 1140–41 (“Security refers to the hybrid scientific and legal inquiry into (1) whether particular implemented systems, products, and processes can successfully defend against all possible third-party attackers in both physical and digital space, and (2) what legal consequences arise when they cannot Privacy refers to the legal and policy inquiry regarding conflicts between (1) what information a person reasonably expects will be or can be collected and used about her (based in part on the legally-binding promises made to her, whose enforceability arises from dictates of either criminal or civil law), on the one hand, and (2) the technical and business reality of possible or actual collection and repurposing by the collector, on the other.”).

103. Sunstein, *supra* note 24, at 216.

104. *Id.* at 217.

105. See Joel Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1323 (2000) (“While each isolated piece of information may have little meaning or risk minimal potential harm to the individual, the aggregate collection takes on an entirely different character. Analyzing the aggregate can reveal patterns of behavior, profiles, and an intimate slice of the lives of individuals, which can be used to categorize and segregate individuals in society.”).

106. Patrick Wintour, *Russian Bid to Influence Brexit Vote Detailed in New US Senate Report*, GUARDIAN (Jan. 10, 2018), <https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report> [perma.cc/4WGK-XYJJ].

online political manipulation.¹⁰⁷ Calling this a crisis of democracy is an understatement.

The dispersed and cumulative nature of online manipulation may point to a collective action problem. Affected individuals or groups may not have an incentive to pursue any form of legal action to redress their harm, but would rather internalize it. This internalization also means that in the absence of any regulation, democracy itself would find it difficult to counter the harms of online manipulation, due to its dispersed and cumulative nature. A solution must account for the collective nature of the harm resulting from online manipulation and its impact on democratic deliberation.¹⁰⁸ Indeed, legal scholars are already exploring many potential legal solutions.¹⁰⁹ Should tort law and class action empower litigants in fighting online manipulation?¹¹⁰ What kind of government regulation should be imposed on social media and other data aggregators?

But online manipulation has a far more troubling characteristic. The collective nature of its harm stems from its scalability, which affects large volumes of individuals and groups. While manipulation itself predates the Internet, its quantitative escalation could lead to more dangerous consequences for democracy as a whole.¹¹¹ This is perhaps best explained by comparing an individual manipulating others in-person to an intelligent technology which makes sense of data and devises ways to manipulate multiple individuals.

Ryan Calo identifies two distinct characteristics that differentiate digital market manipulation from more traditional forms of manipulation—*personalization* and *systemization*.¹¹² According to Calo, the ability to create personalized advertisements through automated or semiautomated systems is

107. Craig Timberg, *Russia Used Mainstream Media to Manipulate American Voters*, WASH. POST (Feb. 15, 2018), https://www.washingtonpost.com/business/technology/russia-used-mainstream-media-to-manipulate-american-voters/2018/02/15/85f7914e-11a7-11e8-9065-e55346f6de81_story.html?noredirect=on&utm_term=.4dc6ad5a8e27 [perma.cc/9W2E-8FJS].

108. See, e.g., McSweeney, *supra* note 27, at 515 (“For example, millions of fake comments were filed with the Federal Communications Commission during its proceeding revising the Open Internet rules . . .”).

109. See Woods, *supra* note 100 (detailing the potential legal responses to Cambridge Analytica).

110. See McClurg, *supra* note 37, at 69 (making the case for a new tort to address the dehumanizing and privacy-invasive practice of data profiling).

111. See generally Brandon Faulkner, Note, *Hacking Into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1098–99 (2007) (“The characteristics of cybercrime have practically eliminated the spatial and temporal restraints that have traditionally limited the quantity of victims and the amount of damages.”).

112. Calo, *supra* note 22, at 1021.

itself novel, leading to the “systemization of the personal.”¹¹³ The significance lies not in the technology itself, but rather in its impact on human-to-human interactions, which is the main justification for legal intervention.¹¹⁴

Political online manipulation could leverage individual weaknesses and unique characteristics to manipulate broader swathes of society and bring about electoral and policy change. Unlike human manipulation, computer program manipulation has “additional advantages over people in that it never tires, has a nearly limitless memory, and can obscure or change its identity at will.”¹¹⁵ These distinct characteristics create a phenomenon that feels different than its predecessor.¹¹⁶ Perhaps with online manipulation, the challenge also becomes its relationship to *source volume*, from which it benefits. Source volume means that an immense amount of data points, even nonpersonal data, on every aspect of our personalities and activities is available simply as a result of Internet economics and new technologies, which enhances the sophistication of online manipulation.

For example, Jonathan Zittrain writes about a form of online political manipulation he calls “digital gerrymandering.”¹¹⁷ Facebook designed a message that attempted to convince users to vote by showing that their friends had already voted. They believed that this message would convince the average person to vote and that it would increase overall voter turnout. Indeed, Facebook discovered that users who received such message were 0.39 percent more likely to vote.¹¹⁸ As many as 60,000 individuals decided to vote as a consequence of that tailored message, and the ripple effect brought another 280,000 voters who did not receive the message to the polls.¹¹⁹ But what if

113. *Id.*

114. See Jack Balkin, *The Path of Robotics Law*, 6 CALIF. L. REV. CIR. 45, 48–49 (2015) (“[W]hat lawyers call ‘technology’ is usually a shorthand for something far more complex. When we talk about ‘technology,’ we are really talking about (1) how people interact with new inventions and (2) how people interact with other people using those new inventions or presupposing those new inventions.”).

115. Calo, *supra* note 22, at 1040.

116. *Id.* at 1022 (“The systemization of the personal may prove different enough from prior selling practices that regulators or courts will seek limits on digital market manipulation, even if they would be hesitant to curtail age-old sales practices like interpersonal flattery. Or, at the very least, digital market manipulation may just feel different enough to justify intervention.”).

117. Jonathan Zittrain, Response, *Engineering an Election*, 127 HARV. L. REV. F. 335, 336 (2014) <https://harvardlawreview.org/2014/06/engineering-an-election/> [<https://perma.cc/93TH-5B9Z>] (defining digital gerrymandering as “the selective presentation of information by an intermediary to meet its agenda rather than to serve its users”).

118. *Id.* at 336.

119. *Id.*; see also John Markoff, *Social Networks Can Affect Voter Turnout, Study Says*, N.Y. TIMES (Sept. 12, 2012), <https://www.nytimes.com/2012/09/13/us/politics/social-networks-affect-voter-turnout-study-finds.html> [perma.cc/89YP-NB5Z].

Facebook had decided to support one candidate over the other and only serve encouraging messages to certain users who are likely to support a particular candidate? Such manipulation raises a very real question about the boundaries of data use, and while this takes the form of experimentation, it nonetheless endangers democracy. In this hypothetical, data-breach notification law may not offer a remedy, since there is no “breach” that the law is concerned with. However, if Facebook was an information fiduciary, Facebook would be under certain obligations which would classify this data use as a breach of the duty of care and loyalty.

Omri Ben-Shahar critiques today’s data economy based on the phenomenon of “data pollution.”¹²⁰ He argues that construing the harms emanating from data misuse as privacy harms on a very individualistic level¹²¹ is an outdated paradigm because today’s data misuse in the form of election interference represents a social harm which affects public interests more than it affects individual privacy.¹²² Ben-Shahar equates this phenomenon to pollution, because emission of data in such harmful ways creates externalities for society at large, representing a failure of private law and suggesting that we may need a legal solution similar to environmental protection law.¹²³

2. *Experimentation*

Several scholars also note that manipulation, at least at this point in time, leads to experiments on human subjects.¹²⁴ This may seem like a farfetched concern, but Facebook and Cornell University researchers engaged in a covert mood manipulation experiment back in 2012.¹²⁵ Through an algorithm,

120. Omri Ben-Shahar, *Data Pollution* 1–51 (U. of Chi. Pub. Law, Working Paper No. 679, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191231 [perma.cc/P462-Z4UD].

121. *Id.* at 3 (“Under the privacy paradigm, the collection of personal data creates various harms to the *individuals* whose data is collected, used, shared, or lost.”).

122. *Id.* at 7–10.

123. *Id.* at 7 (“[One approach to pollution control is] to utilize ex-post devices, to be triggered in the aftermath of harmful data emissions. Like toxic waste releases from industrial production, data spills are rapidly becoming a major social problem of the digital era. Environmental law uses various tools to shift the harm from toxic waste to the emitters, and data pollution law could similarly focus on liability and prevention. While cleanup of spilled data is largely impossible, the harm from the release can be mitigated by post-spill actions and adequate preparedness. And the expected harm can be reduced by a proper system of deterrence. Liability equal to the social cost of spills (punctuated by compulsory liability insurance) would lead to better precautions and self-regulation.”).

124. See Zarsky, *supra* note 85, at 175 (“Yet a third way to articulate the manipulation-based argument is to note that such actions are unacceptable as they amount to human experimentation.”); see also Tamara Pietry, *Advertising as Experimentation on Human Subjects*, 19 *ADVERT. & SOC’Y Q.* (2018).

125. See Adam D.I. Kramer et al., *Experimental Evidence of Mass-scale Emotional Contagion*

Facebook altered the feeds of hundreds of thousands of unwitting users. The users were selected at random to have their feed either display more positive or more negative content.¹²⁶ Those whose feeds displayed more positive content were more likely to be positive in their status updates, and vice versa.¹²⁷ Therefore, this study demonstrated that social media is able to influence the emotional state of its users by affecting the kind of content they get to see.¹²⁸ Though commentators believe that it is not illegal to conduct such experiments, there is a strong allegation that this breached ethical research guidelines by not obtaining proper consent from the experiment subjects (randomly selected Facebook users).¹²⁹

Tamara Piety explains that allowing cutting-edge psychological and technological tools in advertisement is a de facto authorization of “widespread experimentation on human subjects without their consent and with only minimal oversight.”¹³⁰ Piety contends that experimentation on human subjects through online manipulation exposes the subjects to harm.¹³¹ Indeed, manipulation could cause a variety of societal and individual harms—including fear, anxiety, guilt, addiction, sexism, and racism—depending on what data points are exploited.¹³² Despite this, online manipulation is largely experimental and not controlled by current regulation.¹³³ In some cases, these harms may be difficult to show. Nevertheless, even where harm cannot be directly identified beyond a reasonable doubt, online manipulation should still be regulated because such conduct is wrongful and is likely to cause these harms.

Tal Zarsky notes that the strength of the experimentation argument is that it is deontological, meaning that the act of subjecting unwitting humans to an

Through Social Networks, 111 PROC. NAT’L ACAD. OF SCI. 8788 (2014).

126. *Id.* at 8789.

127. *Id.* (“[F]or people who had positive content reduced in their News Feed, a larger percentage of words in people’s status updates were negative and a smaller percentage were positive. When negativity was reduced, the opposite pattern occurred.”).

128. *Id.* (“These results suggest that the emotions express by friends, via online social networks, influence our own moods . . . providing support for previously contested claims that emotions spread via contagion through a network.”).

129. See Charles Arthur, *Facebook Emotion Study Breached Ethical Guidelines, Researchers Say*, GUARDIAN (June 30, 2014), <https://www.theguardian.com/technology/2014/jun/30/facebook-emotion-study-breached-ethical-guidelines-researchers-say> [perma.cc/L3EB-3CWK].

130. Piety, *supra* note 124.

131. *Id.*

132. See *id.*

133. See, e.g., Michelle Meyer, *Everything You Need to Know About Facebook’s Controversial Emotion Experiment*, WIRED (June 30, 2014), <https://www.wired.com/2014/06/everything-you-need-to-know-about-facebooks-manipulative-experiment/> [perma.cc/U9LQ-VG3F] (explaining that Facebook’s research is not covered by federal research regulations).

experiment is wrongful in itself. This is because it disrespectfully treats humans as instruments employed to achieve a certain goal.¹³⁴ Therefore, it is immaterial whether the experiment is successful, unsuccessful, harmful, or harmless. Though humans have been experimental subjects in many covert projects before, both governmental and corporate, the fact that manipulation is becoming personalized and systemized means that this emerging form of experimentation may be uniquely wrongful.¹³⁵ More empirical evidence of direct harms caused by personalized manipulation experiments is likely to emerge, and it may be that the many harms associated with such activity will largely outweigh the benefits.¹³⁶

C. THE EXCEPTIONALISM OF ONLINE MANIPULATION

The exceptional nature of online manipulation has been explored thoroughly in the advertising sector.¹³⁷ Ryan Calo, exploring the concept of market manipulation, was concerned with whether this phenomenon is different from offline manipulation, and whether this difference warrants legal intervention.¹³⁸ It is important to remember that Calo's analysis of market manipulation is slightly different from other forms of online manipulation, since marketing is largely focused on methods of convincing potential customers to purchase goods and services. Therefore, the effects of market manipulation would be, at most, some loss of privacy, consumers paying for products they do not need, or paying extra for a certain brand.¹³⁹ On the individual consumer level, the cost or harm is marginal. This explains why regulators, such as the Federal Trade Commission, have not attempted to address market manipulation.¹⁴⁰

The availability of data on every aspect of our existence exacerbates this scalability and facilitates it. Today, an ever-increasing breadth of personal data is collected by different actors. Social media is learning about our personalities and preferences by looking at what we share and “like,”¹⁴¹ shopping platforms

134. See Zarsky, *supra* note 85, at 175.

135. See *id.* at 175 (calling this form of experimentation “socially unacceptable”).

136. See *id.*

137. See generally Tal Zarsky, *Online Privacy, Tailoring, and Persuasion*, in *PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION* 209–24 (Katherine Strandburg & Daniela Stan Raicu eds., 2006).

138. See Calo, *supra* note 22, at 1020–24.

139. See *id.* at 1024–34.

140. See *id.* at 1002 (“One reason why market manipulation may not have received sustained scrutiny is that its effects, while pervasive, are limited. Maybe a consumer pays a little extra for a product, for instance, or purchases an item on impulse. Thus, both the downside for consumers and, importantly, the upside for firms, have proven only marginal to date.”).

141. See, e.g., Carole Cadwalladr & Emma Graham-Harrison, *How Cambridge Analytica Turned Facebook “Likes” Into a Lucrative Political Tool*, *GUARDIAN* (Mar. 17, 2018),

are tracking our habits and purchasing patterns,¹⁴² and sensor-based gadgets—“the Internet of Things”—are collecting data about us and our environments.¹⁴³ Household items including smartwatches, vehicles, thermostats, locks, refrigerators, and medical devices all collect personal data.¹⁴⁴ The Internet of Things enhances the ability to collect such a vast and rich volume of data points, which are unique in the sense that regular Internet use would not generate the same quantity of sensor data collected by refrigerators, smart watches, thermostats, and so on. This personal information and sensor data about us could provide a very intimate insight into our lives and open it up for abuse, especially as companies like Facebook, Google, and Twitter are selling their user data to third parties.¹⁴⁵ The large volumes of quality sensor data also create an unprecedented ability to better micro-target individuals.¹⁴⁶ As such, this form of nearly flawless microtargeting is far more intrusive and manipulative than ever before, suggesting that it may become fairly easy to manipulate individuals based on an aggregation of data available about every aspect of their lives.

This may be the moment where legal intervention is going to be more necessary than ever before. As Daniel Solove observes, the dynamic nature of the Internet provides much better targeting capabilities as opposed to static

<https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm> [<https://perma.cc/D6NL-T5W5>] (arguing that “likes” are valuable data that could be utilized for manipulation).

142. See, e.g., Michael Reilly, *Google Now Tracks Your Credit Card Purchases and Connects Them to Its Online Profile of You*, MIT TECH. REV. (May 25, 2017), <https://www.technologyreview.com/s/607938/google-now-tracks-your-credit-card-purchases-and-connects-them-to-its-online-profile-of-you> [perma.cc/2Y8R-ST5K]; see also Solove, *supra* note 33, at 1411. But see Joseph Phelps et al., *Privacy Concerns and Consumer Willingness to Provide Personal Information*, 19 J. PUB. POL'Y & MARKETING 27, 27 (2000) (arguing that the high level of consumer privacy concern appears to have had little discernible impact on consumers' shopping behaviors, as most consumers are willing to give up some of their privacy to participate in a consumer society).

143. See generally Bruce Schneier, *Security and the Internet of Things*, SCHNEIER ON SECURITY (Feb. 1, 2017), https://www.schneier.com/blog/archives/2017/02/security_and_th.html [perma.cc/SAU3-UR94].

144. See Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455, 472 (2019) (“IoT devices enable not only data about direct computer use but also data about driving, home heating and cooling, food stored in a refrigerator, pulse and blood pressure, sleep patterns, and much more.”).

145. See, e.g., González, *supra* note 22, at 9.

146. See, e.g., Sara M. Watson, *Russia's Facebook Ads show how Internet Microtargeting can be Weaponized*, WASH. POST (Oct. 12, 2017), https://www.washingtonpost.com/news/posteverything/wp/2017/10/12/russias-facebook-ads-show-how-internet-microtargeting-can-be-weaponized/?utm_term=.95eb1222ab96 [perma.cc/YJW4-MZLQ] (explaining how Russian operatives used algorithms and past behavior to predict and exploit Facebook users' desires and inclinations in the 2016 U.S. presidential election).

mediums like television or magazines.¹⁴⁷ Solove was concerned about the use of targeting for marketing, yet these techniques have now made it into politics as well. This distinct quantitative nature of online manipulation calls for a novel qualitative approach.¹⁴⁸

But consider the following scenario. Online manipulation is far more sophisticated than its offline counterpart, because the offline form is limited by physics, information gaps, and lack of scalability. A salesperson would face limits in the offline world, as she does not know enough about the potential consumer and her personality, she cannot change her own appearance, and she has limited ability to gain trust.¹⁴⁹ However, online manipulation does not have these limitations.

Data obtained in data breaches may facilitate financial fraud, but the same data may also be used for non-financial online manipulation. While certain financial information like credit card numbers could be easily replaced by financial institutions after a breach, this is not the case for personal information misused for manipulation purposes, particularly if such information reflects immutable or quasi-immutable characteristics like sexual orientation, race, nationality, ideology, and more. Since the Internet does not forget, personal data needs a far more protective legal regime to avoid irreversible and long-lasting harm to privacy and autonomy.¹⁵⁰ Needless to say,

147. Solove, *supra* note 33, at 1410 (“This revolution in targeting technology is possible because web pages are not static like magazine pages. They are generated every time the user clicks. Each page contains spaces reserved for advertisements and specific advertisements are download into those spots. The dynamic nature of web pages makes it possible for a page to download different advertisements for different users. Targeting is very important for web advertising because a web page is cluttered with information and images all vying for the users’ attention. Whereas a television commercial is an orderly linear presentation of details, the web page places everything before the user at once.”).

148. In legal literature, increased quantity often affects the qualitative analysis and approach. For example, a similar approach was discussed in the context of Fourth Amendment doctrine, analyzed by Orin Kerr in the aftermath of *United States v. Jones*. See Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012). There, Justice Alito’s concurring opinion suggested that for Fourth Amendment purposes, “long-term GPS monitoring of a car counts as a search even though short-term monitoring does not,” supporting what is called “the mosaic theory.” *Id.* at 313.

149. See Calo, *supra* note 22, at 1021.

150. See Solove, *supra* note 33, at 1412–13 (“As we live more of our lives on the Internet, we are also creating a permanent record of unparalleled pervasiveness and depth. Indeed, almost everything on the Internet is being archived Our online personas—captured, for instance, in our web pages and usenet postings—are swept up as well. . . . But little on the Internet disappears or is forgotten, even when we delete or change the information. The amount of personal information archived will only escalate as our lives are increasingly digitized into the electric world of cyberspace.”); see also Solove & Citron, *supra* note 33, at 758–59 (“The problem with identity theft is that personal data cannot readily be ‘cancelled’ like a credit-card number. Social Security numbers are difficult to change. Other personal data

such illegally obtained data is often widely available on the dark web,¹⁵¹ allowing any potential manipulator to obtain that data and misuse it accordingly.¹⁵² Currently, cybersecurity law provides for remedies relating to financial information, but ignores the emerging forms of data misuse which can be just as threatening, if not more so.

III. DATA-BREACH LAW: SILVER LININGS AND GAPS

Data-breach notification law comprises a patchwork of federal and state statutes that impose a duty to notify affected individuals when their personal information has been compromised.¹⁵³ When a system is breached, the breached entity is required to send out notifications to consumers in accordance with the different state data-breach notification laws. By requiring breached entities to inform consumers, the law enables those affected to mitigate the risks associated with the data leak by pursuing a course of action they deem appropriate or necessary.¹⁵⁴ Creating that sort of public awareness

such as birth date and mother's maiden name cannot be replaced. Biometric data such as fingerprints or eye scans, health information, and genetic data cannot be exchanged. A criminal may obtain a victim's personal data and use it months or years later; the data will still be useful for committing fraud.”).

151. Personal information obtained in data breaches is often sold on websites on the dark web—a section of the internet only accessible with specialist software such as the TOR browser. This personal information most often includes credit card numbers, social security numbers, and financial information, but it may also be information of other kind that can facilitate non-financial manipulation. *See, e.g.*, Kate O’Flaherty, *93 Million Accounts Exposed as Third Data Trove Goes on Sale on the Dark Web*, FORBES (Feb. 18, 2019), <https://www.forbes.com/sites/kateoflahertyuk/2019/02/18/another-93-million-accounts-exposed-as-third-data-trove-goes-on-sale-on-the-dark-web/#2c5f8d521706> [perma.cc/RKA3-3GUQ].

152. *See, e.g.*, Alyssa Newcomb, *Your Identity Is for Sale on The Dark Web for Less Than \$1,200*, NBC NEWS (Mar. 12, 2018), <https://www.nbcnews.com/tech/security/your-identity-sale-dark-web-less-1-200-n855366> [perma.cc/W89Z-AU6V]; *see also, e.g.*, Tomáš Foltyn, *Babies’ Personal Data Hawked on Dark Web*, WELIVESECURITY (Jan. 26, 2018), <https://www.welivesecurity.com/2018/01/26/babies-personal-data-dark-web/> [perma.cc/A4EW-MRDS].

153. Federal data-breach notification law includes statutes like Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act. State data-breach notification law includes all state statutes on the mandatory disclosure of a data breach affecting residents of that state. *See* Sara A. Needles, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 272 (2009); *see generally* Karl D. Belgum, *Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, 24 (1999); *see also* Kosseff, *supra* note 9, at 1011 (creating six categories for the patchwork of federal and state statutes: “(1) data security statutes; (2) data breach-notification statutes; (3) data security litigation through common law and statutory claims; (4) computer hacking laws; (5) electronic surveillance laws; and (6) the Cybersecurity Act of 2015”).

154. *See* Needles, *supra* note 153, at 24.

is immensely important in an area where secrecy and ambiguity are rampant. This is but one area covered by what is often referred to as “cybersecurity law.” Data-breach notification law is used as a case study in this Article, as it represents a microcosm of the different tradeoffs, interests, values, and balances that underlie cybersecurity law.

Under this scheme, residents of different states—California, New York, Texas, and others—will be covered by their own respective statutes, which often differ in some respects.¹⁵⁵ For example, the California statute provides that a breached entity should provide the following sections in the notification—“What Happened,” “What Information Was Involved,” “What We Are Doing,” and “What You Can Do.”¹⁵⁶ However, many other states have no corresponding provision, which could affect whether a notification is effective in dealing with the risk of future manipulation if such sections are not mandated.¹⁵⁷

In the context of manipulation, the law suffers from definitional and substantive shortcomings. These concerns are specific to data-breach notification law, but they can also be found across federal and state statutes and regulations dealing with information security.

The definitional shortcoming is fairly straightforward. Data-breach notification law limits its applicability to compromised *personal information* resulting from a *breach of security*. Since each state has its own statute, these definitions usually vary, but the concepts of *personal information* and *breach* often overlap across many states. This was intended to ensure that only certain irregular events are covered by the law, while others would be outside of the scope of the law’s applicability. It perhaps made sense at the time to provide this limit, but advancements in technology, paired with new forms of data abuse, creates an uneasy reality of impunity in the wake of emerging technologies. In fact, many privacy laws revolve around similar delineations, which creates a systemic vulnerability when it comes to addressing online manipulation.¹⁵⁸

155. For a comparison of all state breach notification laws as of July 1, 2019, see *State Data Breach Notification Laws*, FOLEY & LARDNER LLP (July 1, 2019), <https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws> [https://perma.cc/ZFB9-AGGR].

156. CAL. CIV. CODE § 1798.29(d)(1) (West 2019); CAL. CIV. CODE § 1798.82(d)(1) (West 2019).

157. For example, the Texas statute does not have a corresponding provision. See Identity Theft Enforcement and Protection Act, TEX. BUS. & COM. CODE ANN. §§ 521.001–.152, (West 2017).

158. See generally Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

On the substantive level, data-breach jurisprudence only takes issue with tangible harms stemming from identity theft or fraud. For example, the Supreme Court held that plaintiffs in data-breach litigation need to prove “an invasion of a legally protected interest” that is “concrete and particularized” and “actual or imminent, not conjectural or hypothetical.”¹⁵⁹ Since then, the Courts of Appeals remain divided on the question of harm. Some Circuits recognize that an increased risk of future harm is sufficient to satisfy Article III standing.¹⁶⁰ However, at least two Circuits do not recognize future risk of harm as sufficient for standing.¹⁶¹ While the Supreme Court had the opportunity to resolve this circuit split in a petition for writ of certiorari in the matter of *Zappos.com, Inc. v. Stevens*,¹⁶² it refused to do so and denied the petition.¹⁶³

Along similar lines, the vast majority of state statutes call for a risk-of-harm analysis to determine whether a notification is required under the respective state statute.¹⁶⁴ If there is no risk of harm (usually defined as financial or identity theft harm), the notification requirement is not triggered. While financial fraud and identity theft still represent serious social problems, this approach significantly impedes what data-breach notification law could do in response to online manipulation as well as other serious harms. It is crucial to understand these definitional and substantive difficulties as part of one whole system and contrast them with the growing concerns and phenomena

159. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1543 (2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)).

160. *See, e.g., Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. Appx. 384 (6th Cir. 2016) (holding that increased risk of fraud and identity theft resulting from insurer’s negligent conduct are sufficient to create standing); *Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016) (holding that increased risk of fraudulent charges and identity theft are future injuries sufficient to satisfy Article III standing); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012) (holding that claims of identity theft resulting from data breach are sufficient to create Article III standing).

161. *See Whalen v. Michaels Stores, Inc.*, 689 Fed. Appx. 89 (2d Cir. 2017); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017).

162. *In re Zappos.com, Inc., Customer Data Sec. Breach Litig.*, 888 F.3d 1020 (9th Cir. 2018), *petition for cert. filed sub nom. Zappos.com, Inc. v. Stevens*, 87 U.S.L.W. 3065 (2018) (No. 18-225).

163. Greg Stohr, *Amazon Zappos Rejected by U.S. Supreme Court on Data Breach Suit*, BLOOMBERG (Mar. 25, 2019), <https://www.bloomberg.com/news/articles/2019-03-25/amazon-s-zappos-rejected-by-u-s-high-court-on-data-breach-suit> [perma.cc/67K3-M7VJ].

164. *See* BAKER HOSTETLER, DATA BREACH CHARTS (2018), https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf [perma.cc/9TGQ-APDP] (demonstrating that as many as forty-three state statutes require some form of risk-of-harm analysis to determine whether the notification requirement is triggered).

associated with online manipulation.

A. DEFINITIONAL BOUNDARIES

State data breach notification laws typically revolve around two important definitions. First, whether the compromised information in question is *personal information*, as defined in the statute, and, second, whether the event in question is covered by the statute, i.e., whether it is in fact a *data breach* or *breach of security* as provided in the respective statute.

1. *Personal: Demographic Versus Psychographic*

Different federal and state statutes on information security and privacy contain their own definitions of “personal information.” Data breach notification laws have their respective definitions in each state,¹⁶⁵ as well as in federal legislation such as the Children’s Online Privacy Protection Act,¹⁶⁶ Financial Modernization Act,¹⁶⁷ Fair Credit Reporting Act,¹⁶⁸ Health Insurance Portability and Accountability Act,¹⁶⁹ and the Privacy Act.¹⁷⁰ The definition of “personal information” is similar under each of these legislative regimes in

165. *See, e.g.*, CAL. CIV. CODE § 1798.29 (West 2019) (defining personally identifiable information as:

[an] individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social security number.
- (2) Driver’s license number or California Identification Card number.
- (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
- (4) Medical information.
- (5) Health insurance information).

166. 15 U.S.C. § 6501(8) (2018); 16 C.F.R. § 312.2 (2019) (defining “personal information” as “individually identifiable information about an individual collected online” which among other things, includes first and last name, home address, e-mail address, telephone number, and Social Security number).

167. 15 U.S.C. § 6809(4)(A) (2018) (defining “nonpublic personal information” as “personally identifiable financial information”).

168. 15 U.S.C. § 1681a(d)(1) (2018) (defining “consumer report” as “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living”).

169. 45 C.F.R. § 160.103 (2019) (defining “protected health information” as “individually identifiable health information”).

170. 5 U.S.C. § 552a (1976) (defining “record” as a combination of “education, financial transactions, medical history, and criminal or employment history” and the employee’s “name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph”).

their focus on demographics and plainly identifiable information about the individuals covered by their mandate.

The focus on demographic information as personal information is understandable, as these statutes were enacted long before advanced technologies made psychographic profiling possible. However, today, the tension between demographics and psychographics is very well demonstrated by this narrow approach adopted by data-breach notification law, focusing on whether personal information was accessed or not. It is now obvious that this approach is fundamentally flawed. This is not to say that the protection of demographic information is not important for society as a whole. Rather, data that does not qualify as “personal information” under the law could nonetheless be misused if accessed by unauthorized actors. These actors can then process that data through advanced technologies similar to Cambridge Analytica, which leveraged thousands of data points it obtained on millions of individuals whose information was compromised. As Andrew McClurg aptly put it in this context—“a thousand words are . . . worth a picture.”¹⁷¹ Many tiny data points may create a highly detailed picture about an individual’s life. Jeff Kossseff notes that such nonpersonal information “still may be quite sensitive and valuable to identity thieves or other criminals, but the notification rule does not apply.”¹⁷² Andrea Matwyshyn holds a similar view, in which she argues that legally sensitive information is not necessarily the most valuable kind of information. She argues “[v]alue in information is driven by scarcity, not sensitivity.”¹⁷³ For example, our credit card information may be sensitive, but it is not scarce because of how often we share that information with businesses and other individuals. However, an ice cream preference may not be as sensitive, but it is scarce.¹⁷⁴ After all, how often is that information provided to others? The value of the latter, therefore, may be much higher than a replaceable credit card number.¹⁷⁵ This represents a considerable gap between how the law views sensitive information worthy of protection and

171. McClurg, *supra* note 37, at 70.

172. JEFF KOSSEFF, *CYBERSECURITY LAW* 37–38 (2017).

173. Andrea M. Matwyshyn, *Privacy, The Hacker Way*, 87 S. CAL. L. REV. 1, 15 (2013).

174. *Id.* at 25 (“Perhaps the most essential part of finding value in access to information about my favorite beer and my network of friends, however, rests in its scarcity. The fewer the number of people who know the name of my favorite beer and the identities of my friends, the fewer the number of companies that can market to us with an informational edge. In other words, access to the knowledge of my favorite beer involves information that is subject entirely to my control and derives independent value from not being widely known.”).

175. See Brian Stack, *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Apr. 9, 2018), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> [perma.cc/NJ9Z-5EMT] (reporting that credit card numbers sell for a relatively cheap price on the dark web, ranging from \$5–\$110).

non-sensitive or nonpersonal information that is excluded from its scope.

These notions are further strengthened by Paul Ohm's contention that computer science has demonstrated the capability to "reidentify" and "deanonymize" databases of anonymized personal information.¹⁷⁶ What this means is that our understanding of what constitutes personal and nonpersonal, encrypted and decrypted, and anonymized and deanonymized is immensely outdated. The peril in such anachronism is that a considerable portion of current information privacy law is outdated and dangerously ineffective, requiring a reexamination by lawmakers.¹⁷⁷

Paul Schwartz and Daniel Solove highlighted a similar problem, which they called the Personally Identifiable Information (PII)¹⁷⁸ problem.¹⁷⁹ They determine that the "unstable category" of PII adopted by information privacy law is flawed because it limits the scope of what information is worthy of legal protection.¹⁸⁰ PII is not a category limited to just one statute—rather, it is an overarching theme in all of information privacy and security law, both on the federal and state levels.¹⁸¹ They conclude that the delineations of PII and non-PII should not be abandoned, but instead recommend certain modifications to the PII approach, calling it PII 2.0. PII typically includes information such as first and last name, address, work telephone number, email address, home telephone number, and general educational credentials.¹⁸² This definition still excludes psychographics—personality traits, weaknesses, tendencies, affiliations, and more.

2. *Breach Versus Unauthorized Acquisition*

The definition of "breach of security" in most state data-breach notification laws is based on unauthorized acquisition of personal information.¹⁸³ Like many other state statutes, the California statute defines breach of system security as "unauthorized acquisition of computerized data

176. See Ohm, *supra* note 158, at 1704.

177. See *id.* ("Yet reidentification science exposes the underlying promise made by these laws—that anonymization protects privacy—as an empty one, as broken as the technologists' promises. At the very least, lawmakers must reexamine every privacy law, asking whether the power of reidentification and fragility of anonymization have thwarted their original designs.").

178. See 2 C.F.R. § 200.79 (2019) ("PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.").

179. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1836 (2011).

180. *Id.* at 1816.

181. *Id.*

182. See 2 C.F.R. § 200.79 (2019).

183. See, e.g., CAL. CIV. CODE § 1798.29 (West 2019); see also JOHN HUTCHINS ET AL., U.S. DATA BREACH NOTIFICATION LAW: STATE BY STATE (2007).

that compromises the security, confidentiality, or integrity of personal information maintained by the agency.”¹⁸⁴ Similarly, the U.S. Computer Emergency Readiness Team (US-CERT) defines data breach as the “unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.”¹⁸⁵ However, these statutes should focus on the data compromised, rather than whether an intrusion took place or not. Sara Needles observes that data-breach notification laws apply to a broad set of activities that compromise personal information.¹⁸⁶ A few examples include the physical loss of hardware (such as laptops and USB drives), an individual unintentionally misusing data, insider threat, a vendor inappropriately authorizing use of data, or an external intrusion.¹⁸⁷ This notion makes a lot of sense, considering that the purpose behind the law is to inform consumers that their data is now in the possession of an unauthorized entity. After all, stolen laptops containing sensitive information are not much different than hacking those same laptops.¹⁸⁸

However, many companies have resisted a broader understanding of activities that would trigger data-breach notification laws. These companies push for an interpretation that asks whether an external intrusion—a “hack”—took place.¹⁸⁹ This means that many compromised companies would not be required to inform consumers affected by the data loss unless there is an external actor who intruded on digital assets that include unencrypted personal information.¹⁹⁰

184. CAL. CIV. CODE § 1798.29(f) (West 2017).

185. See *Glossary*, US-CERT (Nov. 28, 2018), <https://niccs.us-cert.gov/glossary> [perma.cc/4K76-T58H] (defining data breach as “[t]he unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information”).

186. See Needles, *supra* note 153, at 274 (listing the many aforementioned examples of data breaches).

187. *Id.*

188. See, e.g., *id.* (noting that the Bureau of Alcohol, Tobacco, Firearms, and Explosives lost hundreds of laptops between 2002 and 2007, many containing classified or sensitive data).

189. See Ido Kirovsky, *The Cambridge Analytica Debacle is Not a Facebook “Data Breach.” Maybe it Should Be*, TECHCRUNCH (Mar. 17, 2018), <https://techcrunch.com/2018/03/17/the-cambridge-analytica-debacle-is-not-a-facebook-data-breach-maybe-it-should-be> [perma.cc/P6UE-HDHG] (“There was no unauthorized external hacking involved, meaning that Facebook databases were not breached by an outside malicious actor. At the same time, this approach misses the point entirely in terms of user privacy and security. It should not matter for a company like Facebook whether their users’ personal information was forcefully obtained through brute-force, or whether Facebook’s personnel were manipulated to hand in that information to malicious and untrustworthy party.”).

190. See Lorenzo Franceschi-Bicchieri, *Why We’re Not Calling the Cambridge Analytica Story a ‘Data Breach’*, MOTHERBOARD (Mar. 19, 2018), <https://motherboard.vice.com/>

This leads to a paradox. The incentives and disincentives provided by information privacy and security law results in malicious actors gaining access to personal information through lawful channels. For example, malicious actors can purchase data or access it through developer-facing platforms.¹⁹¹ This was the case with Cambridge Analytica: even though it purchased the data collected by Facebook, it did so by contacting a developer who had a direct and legitimate channel between his app and Facebook’s *Graph* API.¹⁹² While the actions of Cambridge Analytica did not constitute a breach in the technical sense, as they did not hack or attempt to hack Facebook, it nonetheless was a breach of security in the consequential sense. This is because personal and nonpersonal data about certain Facebook users made its way to unauthorized hands.¹⁹³ This is an important distinction to keep in mind, as Facebook vehemently denied that there was a data breach in the legal or technical sense by claiming that Cambridge Analytica’s unauthorized access to Facebook data “was unequivocally not a data breach” as “no passwords or information were stolen or hacked.”¹⁹⁴ Strategically, it is clear why Facebook chose that rhetorical path, as the regulatory and public-relations’ implications of admitting a breach for any company are staggeringly significant,¹⁹⁵ though Facebook still notified

en_us/article/3kjzvk/facebook-cambridge-analytica-not-a-data-breach [perma.cc/W3ET-RDKG] (“[W]e believe that describing this incident as a breach would . . . mislead our readers No one hacked into Facebook’s servers exploiting a bug, like hackers did when they stole the personal data of more than 140 million people from Equifax. No one tricked Facebook users into giving away their passwords and then stole their data, like Russian hackers did when they broke into the email accounts of John Podesta and others through phishing emails.”).

191. See Nicholas Thompson & Fred Vogelstein, *A Hurricane Flattens Facebook*, WIRED (Mar. 20, 2018), <https://www.wired.com/story/facebook-cambridge-analytica-response/> [perma.cc/DK8E-W8A8] (“The story of how Kogan ended up with data on 50 million American Facebook users sounds like it should involve secret handshakes and black hats. But Kogan actually got his Facebook data by just walking in Facebook’s front door and asking for it. Like all technology platforms, Facebook encourages outside software developers to build applications to run inside it, just like Google does with its Android operating system and Apple does with iOS.”); see also Kilovaty, *supra* note 189.

192. Jonathan Albright, *The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle*, MEDIUM (Mar. 20, 2018), <https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747> [perma.cc/NBV2-VJNG] (“Facebook’s Graph API was a revolution in large-scale data provision. It converted people and their likes, connections, locations, updates, networks, histories, and extended social networks into — quite literally — ‘objects.’ It made the company’s offerings and the data its users generated more economically viable.”).

193. See Kilovaty, *supra* note 7.

194. See Andrew Bosworth (@boztank), TWITTER, (Mar. 17, 2018, 7:38 AM), <https://goodyfeed.com/wp-content/uploads/2018/03/fb-3.png> [perma.cc/UG3M-VV66].

195. See Kate Vinton, *Is It Time to Force Companies to Admit When They’ve Been Hacked?*, FORBES (June 11, 2014), <https://www.forbes.com/sites/katevinton/2014/06/11/is-it-time-to-force-companies-to-admit-when-theyve-been-hacked/#4c7330c5f67a> [https://perma.cc/

its users after the incident was reported by the press.¹⁹⁶

Julie Cohen emphasizes how third parties that gain unauthorized access to data are able to use it in ways that are anything but transparent.¹⁹⁷ She says:

Most reputable firms that deal directly with consumers do disclose some information about their ‘privacy practices,’ but the incentive is to formulate disclosures about both purposes and potential recipients in the most general terms possible. This practice shields secondary recipients of personal data, many of whom do not disclose information about their activities at all.¹⁹⁸

What Cohen means is that while regulators tend to focus their efforts on primary data collectors, such as Facebook and Google, it is often the secondary use of data that lacks transparency and therefore harms the data subjects in uncontrollable ways. This was best exemplified by Facebook (primary data collector) sharing data with Aleksandr Kogan (secondary recipient) who transferred that data to a third party: Cambridge Analytica.

In a sense, data-breach notification law makes the primary data collector solely responsible for data misuse. In some respects, the primary data collector is better situated to provide the transparency and information on what is being done with the data, and more importantly, whether there is a risk or actual occurrence of manipulation down the line. For example, a social media platform whose data is compromised would be able to learn more about the risks, how such data is being misused, and who the perpetrator is, especially as the legal dispute and potential investigation emerges between regulators, social media, and the unauthorized entity. At times, regulatory agencies such as the FTC and SEC may step in with enforcement action, but the expectation is that the collector of the data notify its users of any abnormalities.

B. SUBSTANTIVE SHORTCOMINGS

A major substantive shortcoming in current cybersecurity law, primarily in how it is litigated, is its narrow focus on identity theft as a harm.¹⁹⁹ It is hard

B8XN-U56X] (“Embarrassment and business culture contribute to a lack of transparency in data breach reporting, according to Boyer. The majority of security breaches are accomplished through less-than-sophisticated methods, and companies don’t like admitting to these kinds of attacks.”).

196. Steve Inskeep, *Facebook Will Notify 87M Users Whose Data May Have Been Used By Cambridge Analytica*, NPR (Apr. 5, 2018), <https://www.npr.org/2018/04/05/599997683/facebook-will-notify-87m-users-whose-data-may-have-been-used-by-cambridge-analyt> [perma.cc/WL8H-5YFX].

197. JULIE E. COHEN, *CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE* 235 (2012).

198. *Id.*

199. See Kosseff, *supra* note 14, at 344–45 (“The current patchwork of laws that purport

to imagine a connection between massive online manipulation and identity theft, as the former does not typically lead to the latter. Manipulating Internet users does not require stealing their identity; it simply denotes that particular information about them is being used against them, and identity misrepresentation certainly is not required. This means that in order for data-breach laws to protect consumers and inform them about potential misuse of their personal data by third parties, it needs to expand its purpose to also protect from the risk and harm of manipulation.

1. *Identity Theft Versus Manipulation Harm*

The tension between identity theft and manipulation harm is key to understanding why current cybersecurity law fails to protect consumers from the new threats of the digital medium. It is perhaps best illustrated by how, in thirty-eight states, companies are not required to inform their consumers of a breach if they determine that there is no risk of harm.²⁰⁰ But in that context, what is harm?²⁰¹ Most data-breach case law narrowly focuses on the harm of identity theft and fraud, and therefore “risk for harm” relates solely to identity theft and fraud.²⁰² On that same note, courts have been restrictive in the type of injury that they are willing to recognize and redress as part of data-breach litigation. There may be times where data obtained through a data breach may be used both for identity theft and manipulation, though some data could be insufficiently specific for identity theft, but sufficient to successfully manipulate an individual.

to address cybersecurity are focused largely on preventing economic harms such as identity theft.”).

200. See KOSSEFF, *supra* note 172, at 39 (2017) (“In thirty-eight of the states with breach notification laws, companies can avoid notification obligations if, after investigating the breach, they determine that the incident did not create a risk of harm for individuals whose personal information was exposed.”).

201. For a brief theory of harm discussion, see Catherine Padhi, *Standing in Data-Breach Actions: Injury in Fact?*, LAWFARE (Dec. 18, 2017), <https://www.lawfareblog.com/standing-data-breach-actions-injury-fact> [perma.cc/2DVC-XM4E]. For how the Federal Trade Commission views harm in its data security enforcement action, see Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 639 (2014) (“In evaluating whether a trade practice is unfair, the FTC focuses largely on substantial injury to consumers. Monetary, health, and safety risks are common injuries considered ‘substantial,’ but trivial, speculative, emotional, and ‘other more subjective types of harm’ are usually not considered substantial for unfairness purposes.”). See also Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2279 (2015).

202. See Priscilla Fasoro & Lauren Wiseman, Covington & Burling LLP, *Standing Issues in Data Breach Litigation: An Overview*, INSIDE PRIVACY (Dec. 7, 2018), <https://www.inside-privacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview> [https://perma.cc/ZXK8-T38S].

It is understandable why courts follow this path, though this practice is becoming harder to defend. Why are courts unable to recognize manipulation harm as a redressable harm? It is plausible to say that courts do not view online manipulation as a redressable harm due to its ethereal nature. This concern dates back to Nancy Levit's work on "Ethereal Torts," which are "causes of action for intangible or emotional injuries or deprivations of expectancy or reliance interests, the privacy torts, infliction of emotional distress, breach of confidence, breach of good faith, interference with economic expectancies, loss of a chance, or *loss of choice*."²⁰³ In some cases, courts have been able to award damages based on these intangible and emotional injuries.²⁰⁴ Can a loss of choice be quantifiable for remedy purposes? How about a harm to autonomy, privacy, and democracy?

Legal scholars recognize this inability of courts to grant remedies in cases of privacy harm.²⁰⁵ In her work, Lauren Scholz argues that privacy should be deemed quasi-property, the violation thereof entitling the victim to restitution, which is the "quintessential privacy remedy."²⁰⁶ Scholz argues that courts should focus on the defendant's gain when assessing privacy harms.²⁰⁷ Scholz's work is a demystification of remedies in privacy cases, showing how courts are able to remedy privacy harms. This approach could be extended to remedies in manipulation cases as well, though more scholarly attention would be required for that particular issue.

2. Other Harms

In their seminal article "The Right to Privacy," Samuel Warren and Louis Brandeis recognized that privacy harms may be intangible, but nonetheless be as serious as physical harm.²⁰⁸ They describe individuals who were subjected to privacy harm as experiencing "mental pain and distress, far greater than could be inflicted by mere bodily injury."²⁰⁹ So the notion of intangible harm as a result of a privacy harm is not particularly new. Yet, within the rubric of

203. Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 139 (1992).

204. See, e.g., Robert W. Wood, *Hulk Hogan Settles \$140 Million Gawker Verdict For \$31 Million, IRS Collects Big*, FORBES (Nov. 3, 2016), <https://www.forbes.com/sites/robertwood/2016/11/03/hulk-hogan-settles-140-million-gawker-verdict-for-31-million-irs-collects-big/#310b385e6e84> [<https://perma.cc/P8WE-SY2U>].

205. See Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. (forthcoming 2019), <https://ssrn.com/abstract=3159746> [perma.cc/KA2D-TE2J].

206. *Id.* at 2.

207. See *id.*

208. See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890) ("[M]odern enterprise and invasion have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.").

209. *Id.* at 196.

data-breach litigation, courts tend to favor identity theft harm claims.²¹⁰ Recent scholarship suggests that the scope of harms related to data breaches should be reconsidered, and possibly expanded.²¹¹

Daniel Solove and Danielle Citron recently explored whether harms other than identity theft and fraud should qualify under data-breach notification law.²¹² They ask a provocative question: are risk and anxiety harms protected under data-breach notification law? Solove and Citron explain that courts have been consistent in dismissing lawsuits alleging mere risk of identity theft or emotional distress as a consequence of a data breach under Supreme Court precedent set in *Clapper v. Amnesty International USA*.²¹³ In *Clapper*, the plaintiff alleged that government surveillance programs under the Foreign Intelligence Surveillance Act (FISA) harms journalists, lawyers, and human rights activists by requiring them to increase their spending to secure their communications with foreign entities.²¹⁴ The *Clapper* Court dismissed the lawsuit on the grounds of lack of standing, holding that plaintiffs did not suffer an “injury in fact” as required under Article III of the Constitution.²¹⁵ Solove and Citron note that ever since, courts have held in many cases that the harms alleged were “not concrete or significant enough to warrant recognition.”²¹⁶ Moreover, even where plaintiffs were able to demonstrate the misuse of their data by hackers, courts have refused to accept such claims as they do not relate to identity theft or future financial injury.²¹⁷ However, as demonstrated earlier in this Article, a current circuit split makes Article III standing even more complex and indeterminate.

It should perhaps be a turning point for data-breach notification law, in which we ought to reevaluate what values and interests the law seeks to protect. How can consumers be better informed about the dangers of personal information misuse? And what is the optimal way to reach equilibrium between firms and consumers? Relying solely on narrow dangers such as identity theft and fraud renders legal recourse obsolete in the wake of the advanced technology of manipulation and more nuanced ways to misuse our personal and nonpersonal information.

210. See generally Solove & Citron, *supra* note 39, at 750 (“The trend is that if a person’s personal data has not yet been used to commit identity theft or fraud, then courts find that plaintiffs have suffered no harm.”).

211. *Id.* at 756.

212. *Id.*

213. *Id.* at 740.

214. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 406–07 (2013).

215. *Id.* at 422.

216. Solove & Citron, *supra* note 39, at 741.

217. *Id.* at 750.

IV. DATA-BREACH NOTIFICATION LAW AS AUTONOMY-BREACH LAW

While data-breach notification law is primarily concerned with identity theft as a result of unauthorized acquisition of personal information, this law protects a variety of other interests in practice.²¹⁸ These interests include reducing risk and uncertainty, and bridging the information gap between firms and consumers.

As firms and malicious actors are better geared today to make sense of big data and to misuse this data for political manipulation through automated systems, the collective magnitude of potential autonomy and privacy harms is far greater than many financial frauds resulting from data breaches. For example, if a data breach leaks primarily financial information, the precautionary steps that need to be taken by all actors are pretty straightforward. Firms inform consumers and strengthen their information security practices, while consumers, with the help of their respective financial institutions, replace compromised credit cards, monitor their credit activity, and report any suspicious activity to the authorities.²¹⁹

The steps to remedy financial data breaches are clear, and for the most part, easily quantifiable. But what should firms and consumers be doing when a data breach has only compromised information that could not be used for financial fraud in any way? This is the murky area of cybersecurity law, which current jurisprudence has not yet fully appreciated. At the very least, breached parties should inform their consumers and provide basic precautionary measures to avoid the adverse effects of manipulation.

At first blush, it may seem that data-breach notification law is a nonobvious solution to the problem of online manipulation. After all, it is essentially a law (or more accurately, fifty state data-breach notification statutes) that addresses when and how companies should inform their consumers of a compromise to their personal information.²²⁰ It requires that breached companies send a notice to affected consumers providing that their data was compromised.

218. See Needles, *supra* note 153, at 270–71 (“More than simply combating identity theft and economic harm to individuals, many state data breach notification laws strike a balance between the conflicting effects on consumers and businesses. Analyzing what a breach notification portends implicates these two main parties that, in terms of privacy interests, are at odds with one another. Business interests in monetizing data clash against consumer protection groups’ cry for data privacy.”).

219. Kosseff, *supra* note 9, at 1015 (“Notification requirements might help some customers avoid identity theft and other harms by alerting them of the possible misuse of their personal information.”).

220 See BAKER HOSTETLER, *supra* note 164.

But data-breach notification law has a greater purpose than that. It directly affects the business model of the digital economy players, who collect data on everyone and everything they interact with. Such massive collection, coupled with the potential harm, raises the question of whether these companies owe certain duties of care, loyalty, and confidentiality to their consumers.

Jack Balkin addresses this exact question.²²¹ He asks whether online service providers should have special duties to consumers, given that they collect massive amounts of consumer data.²²² His concern is that the intersection of privacy and the First Amendment may make it difficult to regulate this industry, but he offers some potential reconciliations, including treating data as a commodity,²²³ which would not trigger the First Amendment because commodities are not speech; and distinguishing between collection, analysis, use, disclosure, and sale of data.²²⁴ He proposes that “many online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries toward their customers and end-users.”²²⁵ This means that there would be certain duties attached to information collected by online service providers, which would protect consumers from misuse, disclosure, or other mistreatment of the data collected about them.

In a sense, using data-breach notification law to address online manipulation is an extension of Balkin’s concept of information fiduciaries. This is because it provides another mechanism to address data misuse, which forces online actors to comply with certain important duties owed to their consumers should they experience a data breach. As such, applying data-breach notification law to manipulation would result in four primary positive outcomes for consumers.

First, it would reduce information gaps between consumers and online service providers through informative notifications on potential breaches and manipulations. Second, it would indirectly limit what information online service providers would be willing to collect about their users, as any additional data would expose them to the risk of breach, liability, and public relations consequences, such as the one that Uber attempted to avoid in 2016.²²⁶ Third,

221. See Balkin, *supra* note 28, at 1186.

222. See *id.*

223. See *id.* at 1195–96.

224. See *id.* at 1196.

225. *Id.* at 1186.

226. Mike Isaac et al., *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES (Nov. 21, 2017), <https://www.nytimes.com/2017/11/21/technology/uber-hack.html> [<https://perma.cc/MFP5-V6DZ>] (“Uber disclosed Tuesday that hackers had stolen 57 million driver and rider accounts and that the company had kept the data breach secret for more than a year after paying a \$100,000 ransom. . . . The company tracked down the hackers and pushed

it would open an avenue for victims to sue in court, as the identity theft paradigm would be expanded to include manipulation harms. Fourth, it would allow for regulatory oversight, primarily through state attorneys general. While state attorneys general are already investigating manipulation such as Cambridge Analytica, using data-breach notification law to address online manipulation will provide clearer guidelines and concepts to inform their work.

The subsequent Section discusses these four contributions.

A. REDUCING INFORMATION GAPS

The role of reducing the information asymmetry in the context of online manipulation is central to the definition of manipulation. The act of manipulation is almost always hidden,²²⁷ which enables its efficacy. We are often manipulated because we are not aware that we are being deceived or influenced. Manipulation's weakness, therefore, is sunlight.²²⁸ Its disclosure reduces its power.²²⁹ Sunstein acknowledges that the "idea of manipulation is sometimes taken to imply a lack of transparency, as if something important is being hidden or not being disclosed."²³⁰ There is a feature in manipulation that remains hidden, Sunstein says, but once that feature is revealed, the manipulation dissipates.²³¹ This lack of transparency is an offense to autonomy and dignity.²³²

By disclosing manipulation to potential victims, data holders can preserve or restore individual autonomy and dignity preferably before manipulation even occurs. When companies are breached, and there is a risk of identity theft for their consumers, the law typically requires the company to notify its consumers.²³³ After all, the company in question has direct access to breach-

them to sign nondisclosure agreements, according to the people familiar with the matter.").

227. The literature recognizes forms of manipulations that are not hidden. *See* Sunstein, *supra* note 24, at 231 ("Some acts can be both manipulative and fully revealed to those who are being manipulated. A graphic health warning, for example, is perfectly transparent (and if it is required by regulation, it is even likely to be preceded by a period for public comment, as was the case for the FDA regulation invalidated by *R.J. Reynolds Tobacco Co. v. FDA* (2012)). Subliminal advertising could be preceded by an explicit warning: 'This movie contains subliminal advertising.' If so, it would still count as a form of manipulation.").

228. *See* Romanosky et al., *supra* note 62, at 259 (using the metaphor "sunlight as disinfectant" to refer to disclosure).

229. *Id.*

230. *See* Sunstein, *supra* note 24, at 231.

231. *Id.*

232. *Id.* at 232.

233. *See* Kosseff, *supra* note 9, at 39–40 ("In thirty-eight of the states with breach notification laws, companies can avoid notification obligations if, after investigating the breach, they determine that the incident did not create a risk of [identity theft or fraud] harm for individuals whose personal information was exposed.").

related information that could help consumers reduce the risk of identity theft. The company in question would eventually learn how and who breached their databases, and whether that actor would seek to exploit such data for direct financial gain or for potential manipulation.²³⁴ Regulators, on the other hand, have limited access to such information in the immediate post-breach period. While it is true that a breached company needs to inform regulators of the relevant facts, most of the information related to the breach is in the hands of the breached company. Needless to say, consumers have no knowledge of their own in such a situation, and they rely wholly on what is provided to them by the breached company.

This lack of knowledge and the consumer expectation to be notified is supported by an empirical study carried out by RAND in 2016.²³⁵ In this study, titled “Consumer Attitudes Toward Data Breach Notification and Loss of Personal Information,” RAND explored a series of questions relating to the consumer perception and experience with data breaches affecting them.²³⁶ This study asked respondents of the manner in which they learned about a data breach.²³⁷ The study found that as many as fifty-six percent of respondents first learned of a breach by receiving a notification from the affected company.²³⁸ This means that data-breach notification is still a major factor in reducing information gaps between breached companies and their consumers, and it is an important tool in notifying consumers on how their compromised data may be misused against them, though some information gaps are not addressed by data breach notification. Notifications on possible manipulation can “empower consumers to take action to prevent further—or future—harm” and to provide “greater awareness all around.”²³⁹ However, additional study is needed to determine what consumers would expect to be notified about.²⁴⁰

234. Facebook, for example, did not disclose the fact that Cambridge Analytica misused user data for manipulation. It only became clear that millions of Facebook users’ personal data was compromised after a whistleblower, formerly working with Aleksandr Kogan, blew the whistle on the scandal to its full extent. See Cadwalladr & Graham-Harrison, *supra* note 141.

235. Lilian Ablon et al., *Consumer Attitudes Toward Data Breach Notification and Loss of Personal Information*, RAND CORP. (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf [perma.cc/Z2CH-4YVT].

236. *See id.* at x–xiii.

237. *See id.* at 16.

238. *See id.* at 17.

239. *See id.* at 29.

240. *See id.* at 19 (covering mostly financial and health information, such as credit card numbers, social security numbers, user account information, and more. Data about personality traits, habits, activities, and otherwise nonpersonal information is not covered in the study and remains outside of the traditional scope of data-breach law, which may pose a harm to consumers in the future).

Empirical research also supports the assertion that current data-breach notification laws reduce the likelihood of identity theft.²⁴¹ Consumers can act in a more informed fashion to restore their rights and protect their interests once the information gap is reduced. But there is certainly room for improvement—for example, by incentivizing and educating consumers on their rights and possible courses of action in the aftermath of a data breach.

Overall, the mere knowledge that manipulation could take place as a result of data-breach is invaluable for individuals whose data has been compromised. It may not be enough to inform consumers that their personal information was compromised, but also that such information is likely to be used for manipulation. The reduction of information gaps such as those addressed by data breach notification should be an indispensable part of the struggle to contain the effects of online manipulation.

B. INDIRECT REGULATION OF DATA COLLECTION

Data-breach notification law, if applied to manipulation, could inhibit the collection of every single data point that online actors collect about their respective consumers.²⁴² Storage costs are ever decreasing, meaning that data collectors often collect data before having a concrete use for it.²⁴³ a phenomenon described “data warehousing.”²⁴⁴ This makes economic sense from the perspective of the collector; however, it creates an insurmountable harm to privacy, security, and autonomy, as it becomes a precious data trove for malicious actors to exploit.²⁴⁵ Increasing the cost on data warehousing is likely to decrease the phenomenon, as hoarding companies would not gain as much benefit from it.

241. Romanosky et al., *supra* note 62, at 268.

242. See NAT'L PUB. SAFETY P'SHIP, FAIR INFORMATION PRACTICE PRINCIPLES (FIPPS) IN THE INFORMATION SHARING ENVIRONMENT (ISE) 2 (1974), https://www.nationalpublicsafetypartnership.org/Documents/The_Fair_Information_Practice_Principles_in_the_Information_Sharing_Environment.pdf [perma.cc/PU5W-7YLQ] (“PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose.”).

243. See McClurg, *supra* note 37, at 73 (“Plummeting data storage costs make it economical for corporations to warehouse data for which they have not yet determined a use.”).

244. See Joel Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1323 (2000) (“[D]ata warehousing is the stockpiling of millions of bits of personal information for future analysis.”).

245. See Shaun B. Spencer, *The Problem of Online Manipulation*, U. ILL. L. REV. (forthcoming 2020) (manuscript at 61–62) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341653 [<https://perma.cc/SLN8-M6WE>] (providing an example of a solution to online manipulation focused on, among other things, the collection of data—“if no data can be collected, then there would be no data to build the dossiers used to target and manipulate consumers. Constraining collection, however, would prohibit marketers from many other uses of that data, such as analyzing the practices and preferences of their own consumers”).

This danger persists even in cases of the so-called “anonymized databases,” which remove personal identification, because they have been proven to be “deanonymizable.”²⁴⁶ Paul Ohm advocates limiting data collection as a solution to the ability to reidentify anonymized databases, particularly when information privacy and security law does not recognize such “anonymized” data as protected under the law.²⁴⁷ He suggests that regulators rein in privacy harms “by squeezing and reducing the flow of information in society, even though in doing so they may result in the need to sacrifice . . . values like innovation, free speech, and security.”²⁴⁸ There are many ways in which regulators could do so, some more contentious than others, but certainly covering a broad scope of data under data-breach notification laws would end up limiting what data is being collected by the covered entities.

The best practices of privacy protection, based on the Privacy Act of 1974, have come to be known as the Fair Information Practice Principles (FIPPs). These include “data minimization” as a key principle.²⁴⁹ Minimization means that collection should only take place where “PII . . . is directly relevant and necessary to accomplish the specified purpose(s)” and should only be retained “for as long as is necessary to fulfill the specified purpose(s).”²⁵⁰ While this principle is recognized, it is not legally binding. The way to enhance compliance with that principle is to increase the cost on entities that do not minimize. Therefore, data-breach notification law which covers a broad scope of data would increase the risks and costs on entities that collect information beyond what is required for their operation, as such extraneous information would expose them to legal liability.

The risk of collecting seemingly irrelevant data is also exemplified in the concept of sensor fusion.²⁵¹ Sensor fusion means that sensor data from different devices, combined together, would increase the capacity of making inferences about the user of these devices.²⁵² Scott Peppet explains that “data

246. See Ohm, *supra* note 158, at 1703.

247. *Id.* at 1766.

248. *Id.* at 1706.

249. See HUGO TEUFEL III, DEP’T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM NO. 2008-01 4 (Dec. 29, 2008) https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf [perma.cc/CWF9-EA5Y] (“DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).”).

250. *Id.*

251. See Scott Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 93 (2014) (“[S]ensor fusion’ dictates that the information from two disconnected sensing devices can, when combined, create greater information than that of either device in isolation.”).

252. See Article 29 Data Protection Working Party, 8/2014 Opinion on the Recent Developments on the Internet of Things, (Sept. 16, 2014) at 7 n.6, <https://ec.europa.eu/>

gleaned from various small sensors can be combined to draw much more complex inferences than one might expect” and that data on simple movements, heart-rate, and even the way an individual holds her cellphone can tell us a lot about that person’s mental and emotional state.²⁵³ The sensor fusion problem connects directly to the problem of manipulation using various data points. It is but one phenomenon that makes nonpersonal information useful for a variety of inferences, whether for psychographic profiling or for discrimination.²⁵⁴ Nonetheless, such data is extremely valuable to malicious actors.

Clearly, curtailing data collection by online actors is not a panacea, as data is one of the fuels of innovation. It allows companies to enhance their products, prevent fraud, and provide more tailored services to their customers.²⁵⁵ However, the indirect nature of the impact provided by data-breach notification laws does not directly limit what companies can collect and store, but rather what counts as protected information under the law. Thus, it only increases the likelihood that covered entities will take this factor into account when assessing risks associated with data breaches.²⁵⁶ The broader the scope of personal information, the more likely it is that companies will invest significant resources in securing that information, or perhaps even avoid collecting such data points altogether, as the risk may not be worth the potential benefit.

justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [perma.cc/3K4P-PK7K] (“Sensor fusion consists in combining sensor data or data derived from different sources in order to get better and more precise information than would be possible when these sources are working in isolation.”); see also Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats of Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1005–06 (2016) (“IoT [Internet of Things] is intimately connected to the notion of big data: collecting and storing a large amount and variety of granular data in real time, and using data analytics to reveal insights from these data. Putting together all the data from the device layer in a big data ‘lake’ enables its analysis in the context of other information, helping previously unseen linkages, patterns, and inferences emerge.”); Peppet, *supra* note 251, at 115 (“More personal, perhaps, researchers are beginning to show that existing smartphone sensors can be used to infer a user’s mood; stress levels; personality type; bipolar disorder; demographics (e.g., gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson’s disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement.”).

253. See Peppet, *supra* note 251, at 121.

254. *Id.* at 117.

255. Calo, *supra* note 22, at 1042–43.

256. Solove & Citron, *supra* 39, at 745 (“[T]he very companies being sued for data breaches make high-stakes decisions about cyber security based upon an analysis of risk.”).

C. REMEDYING VICTIMS OF MANIPULATION

Recognizing manipulation based on a data breach as harm would empower plaintiffs to sue in courts to remedy their harm, if such harm indeed materializes beyond mere risk. It would make manipulation a legally cognizable harm, which is a “harm that the law recognizes as worthy of redress, deterrence, or punishment.”²⁵⁷ As the Supreme Court recognized in *Spokeo v. Robins*, such harm could be either tangible or intangible.²⁵⁸ It would effectively create a framework of legally cognizable manipulation, making data breaches costlier for companies. Currently, these data-breach litigation hurdles on plaintiffs do not impose the full potential of costs on the private corporations who have been breached.²⁵⁹

This redress would not only empower breach victims, but also increase overall information security. While the costs of disclosure (disclosure tax) is considered a deadweight loss, a consumer redress would transfer costs between consumers and breached entities, creating an actual incentive for these entities to reduce the externalities caused by data breaches, thus minimizing social cost.²⁶⁰ This would increase information security, minimize harmful data collection practices, and remedy victims in the cases where breach and manipulation would still take place.

D. REGULATORY OVERSIGHT

Section 45 of the Federal Trade Commission Act already empowers the FTC to investigate and pursue legal action against companies who engage in “unfair or deceptive acts or practices in or affecting commerce.”²⁶¹ As the Third Circuit held in *FTC v. Wyndham Worldwide Corp.*, the FTC has an

257. *Id.* at 747.

258. *See Spokeo v. Robins*, 136 S. Ct. 1540, 1549 (2016) (“Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.”).

259. *See* Tal Zarsky, *Data-Breach Harms—Bringing in the Courts, or Leaving them out?*, JOTWELL (Feb. 19, 2019), <https://cyber.jotwell.com/data-breach-harms-bringing-in-the-courts-or-leaving-them-out/> [perma.cc/J6YP-FK5M].

260. *See* Sasha Romanosky et al., *Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal?*, in WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY 26 (2010) (“We find that both disclosure tax and consumer redress cause the firm to increase its level of care, but only the disclosure tax represents deadweight loss, while redress represents a transfer of costs between the consumer and firm. Therefore, only an increase in redress can reduce the externality caused by the data breach. Further, social cost is always decreasing in consumer redress, but if this is small enough, some disclosure tax is necessary to reduce social cost. Therefore, if the firm bears only a small portion of consumer harm, the social planner may be justified in applying (or threatening to apply) additional fines or fees on the firm in order to minimize social cost.”).

261. 15 U.S.C. § 45(a)(1) (2018).

authority under the “unfair” prong to regulate data security.²⁶² This is now largely the source of authority for the FTC to enforce data security laws against companies whose practices are inadequate and result in harm to consumers. This authority also does not contravene the state data-breach notification law framework. Indeed, the U.S. District Court for the District of New Jersey in *Wyndham* explicitly acknowledged that the FTC regulatory authority over data security may “coexist with the existing data security regulatory scheme.”²⁶³ Therefore, on the federal level, the FTC may pursue action against companies whose data security practices are deemed “unfair.”

It is yet to be seen whether the FTC will also confront manipulation, both directly by online service providers and by third parties who obtain access to data through breaches. In particular, the FTC’s ability to enforce cybersecurity practices leading to data breach harms other than identity theft or financial fraud may be constrained. Recently, the Eleventh Circuit in *LabMD v. FTC* held that the FTC needs to be very specific about what it means by “unfair or deceptive” with regard to data security.²⁶⁴ However, this may be an opportunity for the FTC to clarify what harms and threats ought to be protected by cybersecurity law, and perhaps include manipulation within this ambit.

The FTC is, in a sense, a gap-filler because the data-breach law framework pertains, for the most part, to state legislation which focuses on exceptional incidents—data breaches. The FTC is relevant when manipulation is carried out by the primary data collector. An indication of the FTC’s willingness to engage in such enforcement may be strengthened by its institution of a non-public investigation against Facebook in the Cambridge Analytica aftermath.²⁶⁵ In addition, former FTC Commissioner Terrell McSweeney suggested that “the Commission should continue to study the effect of . . . custom audience tools and psychographics . . . to better scope their potential risks and to inform its enforcement.”²⁶⁶ Reevaluating the meaning of data breach in the context of

262. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015) (affirming the district court’s decision that the FTC has authority).

263. *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014).

264. *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1236 (11th Cir. 2018) (“In sum, the prohibitions contained in cease and desist orders and injunctions must be specific. Otherwise, they may be unenforceable. Both coercive orders are also governed by the same standard of specificity, as the stakes involved for a violation are the same—severe penalties or sanctions.”).

265. Press Release, Fed. Trade Comm’n, Statement by the Acting Director of FTC’s Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices (Mar. 26, 2018), <https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection> [perma.cc/99J3-TQQE].

266. See McSweeney, *supra* note 27, at 528 (“Considerations for the agency include whether advanced targeting technologies and tools that are neutral on their face are, in fact, having disparate impacts in violation of civil rights and equal opportunity laws and whether some of the tools are so manipulative that disclosures are ineffective. For example, not much is known

manipulation would better inform the FTC's enforcement practices, as these often derive their authority from existing statutes that reflect the same outdated notions of breach, harm, and personal information.²⁶⁷

But the key point about data-breach notification law in the context of regulatory oversight is that more clarity on how it relates to manipulation could also empower state attorneys general in investigating breaches that could result in manipulation of their respective states' residents. In the immediate aftermath of the Cambridge Analytica scandal, a bipartisan group of forty-one state attorneys general opened an inquiry against Facebook, demanding answers on how their respective residents' data was misused.²⁶⁸ A more coherent approach on the relationship between data breach and manipulation could improve enforcement on the state side.

E. MANIPULATION AND THE FIRST AMENDMENT

Typically, when theoretical and doctrinal research revolves around the regulation of manipulation, or any other use or collection of information by corporations, a difficulty in terms of the First Amendment arises. Some argue that regulating manipulation would be a restriction on free speech, meaning that such regulation could not be possible without being unconstitutional.²⁶⁹ Under this construction, the manipulator has her own speech interests, and the government will need a compelling argument to justify restriction of such manipulative speech.²⁷⁰

The Supreme Court has previously struck down a law passed by Vermont that sought to “restrict the sale, disclosure, and use of pharmacy records that

about whether and how psychographic targeting powered by massive amounts of data and automated technology works. It has variously been described as both ‘powerful enough to influence elections’ and ‘an imprecise science at best and snake oil at worst.’”)

267. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE 1 (2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf [perma.cc/T92P-XXMK] (“The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children’s Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.”).

268. Press Release, John Shapiro, Pa. Attorney Gen., Attorney General Shapiro Leads Bipartisan Coalition of State AGs in Demanding Answers from Facebook (Mar. 26, 2018), <https://www.attorneygeneral.gov/taking-action/press-releases/attorney-general-shapiro-leads-bipartisan-coalition-of-state-ags-in-demanding-answers-from-facebook> [perma.cc/8WSH-VXEZ].

269. See Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000).

270. See Sunstein, *supra* note 24, at 238.

reveal the prescribing practices of individual doctors.”²⁷¹ The Court reasoned that content-based regulation cannot be justified solely on the grounds of “fear that people would make bad decisions if given truthful information,” and therefore, “the State may not seek to remove a popular but disfavored product from the marketplace by prohibiting truthful, nonmisleading advertisements that contain impressive endorsements or catchy jingles. That the State finds expression too persuasive does not permit it to quiet the speech or to burden its messengers.”²⁷²

This is an important hurdle to keep in mind while considering how to tackle online manipulation. However, the arguments advanced by this Article sidestep the First Amendment concern. Primarily, the solution proposed by this Article does not directly restrict speech in the form of the collection or use of information. Rather, it imposes mandatory disclosure of data breaches that are likely to result in manipulation.

Manipulators may claim that their activities are protected by the First Amendment. However, there is a substantial body of law constraining deception.²⁷³ In addition, regulation of false or deceptive commercial speech is permissible in certain circumstances.²⁷⁴ This legitimate regulation may also be appropriate for online manipulation, particularly if we accept that such manipulation often includes deceiving and lying.²⁷⁵

Scholars realize that influencing data subjects is fundamentally different than convincing them, and that the First Amendment doctrine to date cannot withstand the ever-increasing manipulation online.²⁷⁶ The work of Micah Berman suggests that “it will become harder and harder for the courts to ignore the growing disconnect between doctrine and reality . . . the increased use—or misuse—of neuromarketing and sensory marketing research to influence consumers at a nonconscious level is likely to prompt calls for regulation.”²⁷⁷

271. See *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 557 (2011).

272. See *id.* at 577–78.

273. Gregory Klass, *The Law of Deception: A Research Agenda*, 89 U. OF COLO. L. REV. 101, 105 (2018) (defining deception as “an act or omission that wrongfully causes a false belief in another. The law of deception comprises laws designed to prevent, punish, compensate for, or otherwise address deception”).

274. *Id.* at 235 (citing *Va. State Pharmacy Bd. v. Va. Citizens Consumer Council*, 425 U.S. 748 (1976) as an example of regulation of false or misleading speech).

275. *Id.* at 215 (“[I]here is a great deal of work on lies and deception and we can identify an overlap among lying, deceiving, and manipulating.”).

276. Micah Berman, *Manipulative Marketing and the First Amendment*, 103 GEO. L.J. 497, 543 (2015) (suggesting that the government can find an interest in excluding manipulation from First Amendment’s protection, such interest could be (but not limited to): “protecting public health (or other substantial state interests, such as public safety or environmental protection) by preventing consumers from being manipulated into harmful actions”).

277. *Id.* at 546.

This indicates that a shift in First Amendment doctrine is anticipated in the wake of ubiquitous manipulative behavior online. Indeed, the First Amendment provides less protection on the *collection* and *use* of information, as opposed to *sale* and *disclosure*.²⁷⁸ Since manipulation is achieved for the most part through collection and use, it is likely that the First Amendment will not invalidate the regulation of these practices.²⁷⁹

V. CONCLUSION

Online manipulation for political purposes is a dangerous emerging phenomenon which requires the utmost attention of cybersecurity law. The victims of such manipulation are often unaware of its existence, details, and sophistication. As this Article has argued, data-breach notification law is one example of an area where cybersecurity law may be effective in addressing harmful online manipulation by imposing a duty on breached entities to inform potential victims, though by no means this is the only solution to respond to emerging cybersecurity threats. This requires a reevaluation of what cybersecurity law seeks to protect, in light of the emerging threats enabled by new uses of personal data using new tools such as psychographic profiling through machine learning.

Recent indications from federal and state authorities point to an inclination to reconsider cybersecurity law and its applicability to online manipulation. As this Article has outlined, there is much to consider in that context. Immediate legal intervention is desperately needed to enhance our collective privacy, autonomy, and democracy in the information age. However, existing bodies of cybersecurity law, such as data-breach notification law, can achieve this goal until a more comprehensive and direct regulatory approach is ultimately adopted.

278. Balkin, *supra* note 28, at 1194.

279. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1182 (2005).

SECRECY & EVASION IN POLICE SURVEILLANCE TECHNOLOGY

Jonathan Manes[†]

ABSTRACT

New technologies are transforming the capabilities of law enforcement. Police agencies now have devices to track our cellphones and software to hack our networks. They have tools to sift the vast quantities of digital silt we leave behind on the Internet. They can deploy “big data” algorithms meant to predict where crimes will occur and who will commit them. They have even transformed the humble closed-circuit video camera—and its more recent companion, the body camera—into biometric tracking devices equipped with artificial intelligence meant to pick faces out of a crowd and, eventually, to mine gigabytes of stored footage to automatically reconstruct the movements of their targets.

These kinds of novel police technologies test the constitutional limits on surveillance and raise profound questions about privacy, personal freedom, and potential abuse. Yet the government shrouds them in secrecy. Even as new surveillance tools transform the relationship between people and the police, the public is often left in the dark about how police use these tools and the rules, if any, that govern them. What justifies this secrecy?

This Article examines the primary argument offered by law enforcement in the United States: that disclosure of police technologies would allow criminals to evade the law. Without secrecy, the argument goes, criminals could circumvent law enforcement’s tools, crime would go undetected, and society would suffer the consequences. I call this the anti-circumvention argument for secrecy. This Article is the first to examine it.

The Article contends that the anti-circumvention argument, as currently implemented in law, is producing far more secrecy than it can justify, and that it is doing so at the expense of democratic checks, public accountability, and perhaps law enforcement itself. The Article proposes specific reforms to circumscribe laws that currently authorize excessive secrecy in the name of preventing evasion. The Article also proposes structural changes to require police to publish information about novel technologies for public notice and comment, in order to allow meaningful democratic deliberation as we enter the age of digital policing.

DOI: <https://doi.org/10.15779/Z38NP1WJ7K>

© 2019 Jonathan Manes.

[†] J.D. Yale Law School; M.Sc. London School of Economics; B.A. Columbia University. Associate Professor of Law, University at Buffalo School of Law, State University of New York; Affiliated Fellow, Yale Law School Information Society Project. The author is grateful for detailed feedback on prior drafts from Hannah Bloch-Wehba, Kiel Brennan-Marquez, Hon. Stephen Wm. Smith, Matthew Steilen, and Rebecca Wexler, as well as generous comments from Guyora Binder, Luis Chiesa, Jeremy Epstein, Andrew Ferguson, Jim Gardner, Clare Garvie, Jim Graves, Heidi Kitrosser, Keir Lamont, Laura Moy, Jim Milles, Eduardo Schnadower Mustri, Athena Mutua, Peter Ormerod, Brian Owsley, Christopher Slobogin, David Schulz, Rick Su, Kathy Strandburg, and participants in the Yale Freedom of Expression Scholars Conference, the Privacy Law Scholars Conference, and the University at Buffalo School of Law Faculty Workshop.

TABLE OF CONTENTS

I.	INTRODUCTION	504
II.	THE LIFE CYCLE OF SECRECY IN LAW ENFORCEMENT TECHNOLOGIES	511
A.	THE SAGA OF STINGRAY SECRECY.....	513
B.	THE MYSTERY OF MOBILE X-RAY VANS	520
III.	THE PROBLEM WITH SECRET LAW ENFORCEMENT TECHNOLOGIES.....	524
A.	SECRECY IMPEDES THE ABILITY OF COURTS TO ADJUDICATE THE LEGAL LIMITS WITHIN WHICH NEW TECHNOLOGIES MAY BE USED	524
B.	ANTI-CIRCUMVENTION ARGUMENTS MILITATE AGAINST LEGISLATIVE ENACTMENTS THAT LIMIT HOW NEW TECHNOLOGIES MAY BE USED	527
C.	NEW TECHNOLOGIES AND OLD LAWS PRODUCE UNACCOUNTABLE SELF-REGULATION BY POLICE.....	529
D.	SECRET TECHNOLOGIES RECONFIGURE THE RELATIONSHIP BETWEEN CITIZEN AND STATE	533
E.	SECRECY IMPOSES COSTS ON LAW ENFORCEMENT TOO.....	537
IV.	THE LOGIC OF ANTI-CIRCUMVENTION SECRECY	538
V.	ANTI-CIRCUMVENTION DOCTRINES	546
A.	THE FOIA EXEMPTION FOR LAW ENFORCEMENT “TECHNIQUES AND PROCEDURES”	546
B.	THE EVIDENTIARY PRIVILEGE FOR LAW ENFORCEMENT INVESTIGATIVE TECHNIQUES	552
VI.	REFORMING THE LAW OF SECRET LAW ENFORCEMENT TEHNOLOGIES.....	557
A.	NARROWING THE SCOPE OF ANTI-CIRCUMVENTION SECRECY	558
B.	PUBLIC NOTICE AND COMMENT FOR NOVEL INVESTIGATIVE TECHNOLOGIES.....	562
VII.	CONCLUSION	566

I. INTRODUCTION

Over the last generation, we have seen remarkable innovations in technology that are transforming the investigative powers of the police. The cell phone has radically expanded our communication networks, the Internet has transformed our information infrastructure, social life is increasingly lived

online, and networked computers now operate inside even the most mundane household appliances. These pervasive technologies produce a huge amount of digital information about each of us.

Alongside each of these innovations are parallel developments in law enforcement's ability to conduct investigations and surveillance. The public's mass adoption of digital communication technologies has created enormous new investigative targets. At the same time, police and private vendors have harnessed technological innovations to create new and previously unimaginable investigative tools.

A few examples illustrate the scope and ambition of these technologies. Law enforcement now has ready access to: cell site simulators (aka "Stingrays") that can pinpoint the location of cell phones, log calls, and sometimes even intercept the content of conversations;¹ computer hacking and surveillance software that can surreptitiously hijack and search computers, cell phones, and myriad other Internet-connected devices;² automated license plate readers that track vehicle locations over months or years;³ mobile x-ray vans that scan inside cars and underneath clothing;⁴ facial recognition algorithms that promise to automatically identify individuals in photos or videos, allowing police to track people in real time or to mine gigabytes of stored footage captured by closed-circuit television cameras, police body-worn cameras, or other video sources;⁵ social media data mining tools that generate associational

1. See Stephanie K. Pell & Cristopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy*, 28 HARV. J. LAW & TECH. 1, 8–13 (2014).

2. See generally Privacy International, *Government Hacking and Surveillance: 10 Necessary Safeguards* (2017).

3. See, e.g., *Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND. (last visited Mar. 9, 2019), <https://www.eff.org/pages/automated-license-plate-readers-alpr> [<https://perma.cc/D5L3-T8C6>]; Russell Brandom, *Exclusive: ICE is about to start tracking license plates across the US*, VERGE (Jan. 26, 2018), <https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions> [<https://perma.cc/9QJC-QDFC>]; *You Are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements*, ACLU (2013), <https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf> [<https://perma.cc/MBA2-478E>].

4. See, e.g., *Grabell v. N.Y.C. Police Dep't*, 139 A.D.3d 477, 477–79 (N.Y. App. Div. 2016); Michael Grabell, *Drive-by Scanning: Officials Expand Use and Dose of Radiation for Security Screening*, PROPUBLICA (Jan. 27, 2012), <https://www.propublica.org/article/drive-by-scanning-officials-expand-use-and-dose-of-radiation-for-security-s> [<https://perma.cc/JYF3-Y6LF>].

5. See generally Clare Garvie et al., *The Perpetual Lineup: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf> [<https://perma.cc/TDP9-S7R8>].

graphs, “threat ratings,” and myriad other profiles;⁶ and “big data” artificial intelligence and machine learning tools that purport to predict crime patterns, recidivism risks, or individual security threats based on analyses of massive data sets.⁷ Each of these technologies gives the police new and powerful capabilities to monitor people. Many of these tools raise troubling concerns about personal privacy.⁸ Some tools threaten to reinforce or exacerbate existing racial disparities in policing.⁹ Most of them operate in secret, without the knowledge or consent of targeted individuals and, often, without the ability to challenge how law enforcement uses them. Indeed, the fruits of tech-enabled surveillance, stored in massive databases, can amount to virtual time machines, allowing the police to reconstruct a person’s comings and goings and communications going back months or years.¹⁰ Clearly, these technologies raise profound questions about how law enforcement uses them and how they should be regulated.

6. See, e.g., MOHAMMAD A. TAYEBI & UWE GLÄSSER, SOCIAL NETWORK ANALYSIS IN PREDICTIVE POLICING 7–14 (2016); Brent Skorup, *Cops scan social media to help assess your ‘threat rating’*, REUTERS: GREAT DEBATE (Dec. 12, 2014), <http://blogs.reuters.com/great-debate/2014/12/12/police-data-mining-looks-through-social-media-assigns-you-a-threat-level/> [<https://perma.cc/UY3E-ZREK>].

7. See generally Andrew G. Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259 (2012); Elizabeth Joh, *Artificial Intelligence & Policing: First Questions*, 41 SEATTLE U. L. REV. 1139 (2018); Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy’s Perfect Storm*, 19 J. TECH. L. & POL’Y 105 (2014); Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871 (2016); see also Ava Kofman, *Taser Will Use Police Body Camera Videos “To Anticipate Criminal Activity”*, INTERCEPT (Apr. 30, 2017), <https://theintercept.com/2017/04/30/taser-will-use-police-body-camera-videos-to-anticipate-criminal-activity/> [<https://perma.cc/B987-W53U>]; Doug Wylie, *What TASER’s acquisition of 2 AI companies means for the future of policing*, POLICE ONE (Feb. 9, 2017), <https://www.policeone.com/police-products/less-lethal/TASER/articles/289203006-What-TASERs-acquisition-of-2-AI-companies-means-for-the-future-of-policing/> [<https://perma.cc/UTG2-EE75>]; Axon Int’l, *Law Enforcement Technology Report 21–31* (2017), <https://www.documentcloud.org/documents/3679537-Taser-2017-Law-Enforcement-Technology-Report.html> [<https://perma.cc/3U4V-V5VN>].

8. See, e.g., ACLU, COMMUNITY CONTROL OVER POLICE SURVEILLANCE: TECHNOLOGY 101 (2016), https://www.aclu.org/sites/default/files/field_document/tc2-technology101-primer-v02.pdf [<https://perma.cc/A6HZ-7DFM>].

9. See, e.g., Garvie et al., *supra* note 5; Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, ATLANTIC (Apr. 22, 2016), <https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/> [<https://perma.cc/9BDJ-933Q>].

10. See generally Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773 (2015). The Supreme Court has recognized the Fourth Amendment concerns raised by technology that allows “the Government [to] travel back in time to retrace a person’s whereabouts.” *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (holding that collection of seven days of cell-site location information from a wireless carrier is a search under the Fourth Amendment and requires a warrant).

Alarming, however, in the United States these new capabilities have proliferated largely in secret. At best, disclosure is significantly delayed with respect to new police technologies, their uptake by particular agencies, the policies governing their use, and the manner in which they are being deployed. These innovations thus threaten to radically reorient the informational balance of power between citizens and the state, giving law enforcement ready access to enormously detailed and intimate data about people's lives, while leaving the public in the dark about the police's capabilities. This secrecy is no accident. In many instances, government agencies have actively and vigorously resisted disclosure of any official information about their new technological capabilities and the rules governing their use.¹¹

What explains this degree of secrecy? The principal justification offered by the law enforcement community has been powerful and simple: we must keep our methods secret in order to prevent criminals from circumventing our investigative techniques. Without secrecy, the argument goes, criminals would be able to evade law enforcement's tools, crime would go undetected, and society would suffer the consequences.

I call this the anti-circumvention argument for secrecy. This Article is the first to examine the argument in depth and to analyze the legal doctrines that instantiate it.¹²

11. See *infra* Sections II.A–B.

12. The other argument often advanced to keep information about law enforcement technology secret is that disclosure would impair business confidences or trade secrets. At first blush, this rationale seems entirely out of place in the context of public police forces. But the argument arises because, increasingly, law enforcement agencies purchase their advanced investigative tools from private companies. Such companies argue (or the police argue on their behalf) that disclosure of information about the tools would cause competitive harm or impair trade secrets.

Three excellent recent papers focus on the trade secrecy rationale for secrecy of police technologies. See generally Natalie Ram, *Innovating Criminal Justice*, 112 NW. L. REV. 659 (2018); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018); Eli Siems & Katherine J. Strandburg, *Trade Secrets and Markets for Evidential Forensic Technology*, (May 14, 2018) (unpublished manuscript) (on file with author). The purchase of private technology by police also raises policy concerns beyond secrecy, including questions about who controls, regulates, and sets policy for use of these technologies. Professors Catherine Crump and Elizabeth Joh, among others, have written incisively about these issues. See generally Catherine Crump, *Surveillance Policymaking by Procurement*, 91 WASH. L. REV. 1595 (2016); Elizabeth Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. 102 (2017).

While this Article develops a number of anti-secrecy arguments that might be deployed against the business confidentiality/trade secret arguments, I do not engage directly with that issue here. This Article is focused instead on the anti-circumvention rationale for secrecy, which constitutes a separate, little-examined obstacle to transparency and accountability—one that that would persist even if concerns about outsourced technology were overcome.

The anti-circumvention argument begins from the premise that if law enforcement discloses certain information about its technological capabilities or how it uses them, then lawbreakers—particularly terrorists, drug trafficking organizations, and other sophisticated criminals—will learn how to avoid detection, interdiction, and prosecution. Such criminals will be able to exploit the gaps in both the capabilities of law enforcement’s technologies and the manner in which they are deployed. They will, as a result, be able to wreak havoc unimpeded and evade apprehension at will.

The Federal Bureau of Investigation (FBI) has made this argument in particularly stark and ominous terms, raising the specter of large numbers of kidnappings and murders going unpunished. A sworn affidavit from the head of its Tracking Technology Unit made the case for secrecy with respect to information about cell-site simulator devices.¹³ The FBI official warned, “discussion of the capabilities and use of the equipment . . . could easily lead to the development and employment of countermeasures” and “completely disarm law enforcement’s ability to obtain technology-based surveillance data in criminal investigations,” thereby “completely prevent[ing] the successful prosecution of a wide variety of criminal cases involving terrorism, kidnappings, murder, and other conspiracies where cellular location is frequently used.”¹⁴

Versions of this anti-circumvention argument have also been made outside the criminal law enforcement context. For example, the Internal Revenue Service (IRS) will not disclose the “checklist used by agents to detect fraudulent tax schemes”¹⁵ or the precise specifications that it uses to automatically flag returns for an audit.¹⁶ Disclosing those flags would give tax fraudsters a roadmap to avoid detection. Similar arguments have been featured prominently in debates regarding the National Security Agency’s (NSA) surveillance activities. For instance, the NSA vigorously resisted disclosing the rules governing its treatment of information about “U.S. persons” on the grounds that doing so would imperil “sources and methods” of intelligence.¹⁷

13. See Affidavit of Bradley S. Morrison, Chief, Tracking Technology Unit, FBI (Apr. 11, 2014), <https://www.documentcloud.org/documents/1208337-state-foia-affidavit-signed-04112014.html> [<https://perma.cc/8BCN-KB3R>] [hereinafter Morrison Affidavit].

14. *Id.* at 2.

15. *Mayer Brown LLP v. Internal Revenue Serv.*, 562 F.3d 1190, 1192 (D.C. Cir. 2009).

16. See *IRS Audits*, INTERNAL REVENUE SERV. (Nov. 30, 2017), <https://www.irs.gov/businesses/small-businesses-self-employed/irs-audits> [<https://perma.cc/P878-FDNM>] (describing in general terms the “random selection and computer screening” process for selecting return to audit based on a “statistical formula”).

17. See, e.g., *Al-Haramain Islamic Found. v. Bush*, 507 F.3d 1190, 1195 (9th Cir. 2007); *ACLU v. FBI*, 59 F. Supp. 3d 584, 594 (S.D.N.Y. 2014).

But even though this type of argument has become part of the government's ordinary vernacular in discussions of law enforcement—and it has now been litigated in court numerous times—the argument has not been subject to sustained scrutiny in the scholarly literature.

This Article seeks to fill that gap.¹⁸ It is the first to take a close look at the anti-circumvention argument for secret police technologies. In broad outline, the Article defends three claims.

First, I contend that even if the anti-circumvention argument is sound on its own terms, there are powerful countervailing arguments that militate strongly in favor of transparency with respect to law enforcement innovation.¹⁹

In particular, secrecy undermines institutional checks on the police by other branches of government. Secrecy impedes the ability of the courts to consider and adjudicate compliance with constitutional and statutory limitations because litigants will frequently be unable to mount court challenges to concealed techniques. Secret techniques are also largely immune from legislative oversight and regulation. Even if legislators themselves learn about the police's technologies and the policies that govern them—which is not always a given—oversight is severely weakened in the absence of public disclosure. Indeed, secrecy undermines the accountability of police technologies to the public at large, limiting the ability of citizens to use the levers of democracy to control their law enforcement agencies.²⁰

It is cliché to say that information is power, but when police limit the flow of information about their technical capabilities, it does indeed lead to a troubling concentration of authority. Secrecy produces, in effect, a self-regulatory regime in which law enforcement agencies write their own rules, behind closed doors, about how they can deploy technologies. Even if the secrecy surrounding a technology eventually erodes, as it tends to do over time, the rules and practices that law enforcement has developed over time will enjoy all the advantages of incumbency.

Perhaps even more alarmingly, the anti-circumvention rationale for secrecy militates against the adoption of public rules at all. After all, to make public rules governing a technology's use is to disclose limits on how the technology may be used. According to the anti-circumvention argument, the disclosure of such limits is precisely the kind of information that should not be disclosed, lest criminals develop countermeasures. Seen in this light, public rules, statutes,

18. *See supra* note 12 (describing existing literature on secrecy of law enforcement technologies).

19. *See infra* Part III.

20. *See generally* Barry Friedman, UNWARRANTED: POLICING WITHOUT PERMISSION (2017) (offering a vivid and sustained argument for democratic supervision of policing and the crucial role of secrecy in impeding such oversight).

and judicial opinions are the kinds of disclosures that threaten to permit circumvention of novel law enforcement capabilities. The anti-circumvention argument thus tends to favor keeping the governing rules secret, if they even exist at all. This creates a deep tension with basic liberal and democratic commitments against secret law: public rules governing police are a key protection for individuals against the arbitrary exercise of power.²¹ Put more strongly, a system in which investigatory powers are governed by secret rules is more characteristic of a police state than a democracy such as ours.²²

Moreover, keeping technologies secret can, paradoxically, undermine a law enforcement agency's effectiveness. Disclosure permits input and advice from outside experts. It encourages officials to deliberate carefully about how to deploy technologies most effectively. It permits sharing of best practices among separate agencies. It builds trust between the police and the communities they serve. Indeed, public opposition to new police technologies may be attributable as much to the secrecy of such techniques as it is to their intrusiveness. This dynamic is especially the case with modern investigative technologies that can be deployed without any obvious physical footprint and directed against particular individuals without their knowledge. As Chief Justice Burger wrote in another context, "[p]eople in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing."²³

The upshot of these arguments, and others developed in this Article, is that the anti-circumvention concerns alone hardly settle the question in favor of secrecy. Even if the anti-circumvention argument is sound, accepting it may come at an unacceptable cost.

Second, this Article unpacks the structure of the anti-circumvention argument for secrecy and evaluates its strength.²⁴ Anti-circumvention arguments rest on empirical claims about the consequences of disclosure that are often simply assumed to be true without meaningful scrutiny. Will disclosure actually impair law enforcement's techniques or procedures? Or will it in fact have little to no effect because of other facts already in the public

21. For example, we do not keep Fourth Amendment law secret because police investigatory methods would be more effective if would-be criminals did not know the constitutional limits that police officers are bound to respect.

22. I elaborate on the idea that secret rules are threats to individual liberty in other work evaluating the phenomenon secret law. *See generally* Jonathan Manes, *Secret Law*, 106 GEO. L.J. 803 (2018). For present purposes, the key point is that adopting the anti-circumvention argument can raise secret law concerns because disclosing (or publicly adopting) laws that limit police techniques may create opportunities for circumvention.

23. *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 572 (1980) (holding that the Constitution guarantees the public the right to access criminal court proceedings).

24. *See infra* Part IV.

domain? Will disclosure result in changes in criminal behavior that frustrate enforcement objectives? Or could it instead channel criminal behavior into less socially harmful activities, or deter criminality outright? By taking the argument seriously on its own terms, this Article aims to clarify the internal power and limits of the anti-circumvention argument.

Third, this Article examines the existing legal regimes that empower police to keep their capabilities and techniques secret.²⁵ I conclude that these doctrines permit far more secrecy than the anti-circumvention argument can justify. In particular, both the Freedom of Information Act's (FOIA) exemption for law enforcement "techniques and procedures" and a common-law evidentiary privilege against disclosure have been interpreted to permit an expansive ambit for secrecy. These sources of law provide law enforcement a shield against disclosure that is much stronger than what is required by the logic of anti-circumvention. And neither source of law takes into consideration the countervailing interests favoring disclosure to the public.

The Article concludes by offering proposals for reform.²⁶ In particular, I advocate framework legislation that would require public deliberation about new technologies through the legislature *before* police put them into regular use. I also propose doctrinal changes that would rein in expansive warrants for secrecy under the FOIA and the law enforcement privilege.

The Article proceeds in five parts. Part II illustrates the anti-circumvention argument in action by describing two contemporary examples of secret innovation in law enforcement technology: cell-site simulators and mobile x-ray vans. Part III explores the reasons that secrecy regarding techniques and procedures is often unwarranted, even where anti-circumvention concerns may accompany disclosure. Part IV unpacks the anti-circumvention argument on its own terms, probing its analytic and empirical underpinnings. Part V contrasts this analysis of the anti-circumvention rationale with the legal doctrines that have implemented it in overbroad ways. Part VI offers prescriptions for how to tame the anti-circumvention argument and ensure that excessive secrecy does not thwart democratic deliberation over new, intrusive, and potentially transformative police technologies.

II. THE LIFE CYCLE OF SECRECY IN LAW ENFORCEMENT TECHNOLOGIES

In order to understand how the anti-circumvention argument works in practice, it is essential to closely examine particular examples. This Part focuses on Stingrays and mobile x-ray vans. Because of the privacy concerns that both

25. *See infra* Part V.

26. *See infra* Part VI.

of these technologies raise—and the public health concerns raised by the latter—they vividly illustrate what is at stake when police technology is kept secret and insulated from democratic accountability.

Stingrays and x-ray vans also illustrate the secrecy dynamics that typify innovations in police technology. These technologies typically follow an arc: when they first come into use, they are almost completely opaque to the public. Eventually—often after many years or even decades—they generally come to light and are sometimes then subjected to legal regulation by courts and legislatures. The story usually goes something like this: A law enforcement agency adopts a novel technology and shrouds it in a great deal of secrecy. The agency seeks to maintain this secrecy as long as possible. Information about the technology comes into the public domain slowly, in fits and starts, usually by way of investigative work of technical experts, specialist journalists, or criminal defense teams. Efforts by civil society organizations to force official disclosure through the courts are typically met with powerful legal resistance by the government. Until there is a critical mass of public disclosure and public awareness, courts and legislatures generally do not publicly weigh in on the constitutional or statutory limits on the police’s use of the novel technology. Consequently, law enforcement will typically have put a novel technology into routine use long before it becomes subject to any consistent, public legal framework governing its operation.

The Stingray and x-ray van examples also illuminate how the government employs the anti-circumvention argument in practice to delay disclosure. The government has several legal tools at its disposal, including the FOIA exemptions²⁷ and the evidentiary privilege already mentioned.²⁸ The government also has tools for concealing technologies in the context of criminal prosecutions, including writing warrant applications that obfuscate²⁹ or affirmatively misrepresent³⁰ the technology in question; engaging in “parallel

27. 5 U.S.C. § 552(b)(7)(E) (2018). The FOIA exemption is discussed in detail *infra* Section V.A.

28. See Stephen Wm. Smith, *Policing Hoover’s Ghost: The Privilege for Law Enforcement Techniques*, 54 AM. CRIM. L. REV. 233, 245–46 (2017). The law enforcement privilege is discussed in detail *infra* Section V.B.

29. See *United States v. Patrick*, 842 F.3d 540, 546 (7th Cir. 2016) (“[I]n this case, the government appears to have purposefully concealed the Stingray’s use from the issuing magistrate, the district court, defense counsel, and even this court. It ultimately admitted its use of the device only in response to an *amicus curiae* brief filed during this appeal.”).

30. See, e.g., *id.* at 548 (local police department used Stingray device after obtaining court order that “[a]pprove[d] the release of information,” [from telephone service provider] not the use of a device that would allow the [local police] to track [the suspect’s] phone on its own”); *United States v. Temple*, No. 15-CR-230-1 JAR (JMB), 2017 WL 7798109, at *33 (E.D. Mo. Oct. 6, 2017) (assessing an instance where a cell-site simulator was used and the “application and Court Order d[id] not specifically mention the use of a Cell Site Simulator”).

construction” to hide a secret method by conducting a parallel, clean investigation that “discovers” evidence already identified with a secret technique;³¹ or even dropping criminal charges rather than having to disclose a method and face a challenge to its legality.³²

Stingrays and x-ray vans vividly illustrate these secrecy dynamics. The story is the same, in broad outline, with respect to computer hacking tools, predictive policing software, automated license plate readers, facial recognition technology, and others. Each finds itself at some point along the uncertain arc from secrecy to public disclosure and democratic regulation. I have chosen these two particular examples because they are both far enough along this path to be able to tell an instructive story.

A. THE SAGA OF STINGRAY SECRECY

Stingrays are portable electronic devices that mimic cell phone towers. They force mobile phones within range to connect to the device, rather than the genuine cell tower.³³ While these devices vary in their capabilities, all such devices are capable of logging the identifying information of cell phones nearby.³⁴ Police can also use these devices to triangulate the location of devices (and, therefore, their owners) with a great deal of precision. Many models can precisely track a particular cell phone even if the phone is not actively transmitting voice or data.³⁵ Some models allow users to log details about the calls that each cell phone makes, including the incoming or outgoing phone number and duration of the call. Certain advanced models even permit interception and decryption of the *content* of phone calls and text messages.³⁶

For decades, experts have known that Stingrays exist. The devices exploit vulnerabilities in our cell phone networks that have been well known for twenty years, including the fact that phones will connect to any cell tower, even a spoofed tower, without authentication and that communications are

31. See, e.g., Amanda C. Grayson, Note, *Parallel Construction: Constructing the NSA Out of Prosecutorial Records*, 9 HARV. L. & POL'Y REV. S25, S32–33 (2015); Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1042–43 (2014); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants & The Right to Notice*, 54 SANTA CLARA L. REV. 843, 853–64 (2014).

32. See *Patrick*, 842 F.3d at 546 (“Until recently, the government has gone so far as to dismiss cases and withdraw evidence rather than reveal that the technology was used.”); see also *infra* notes 43, 51 and accompanying text.

33. This descriptive discussion relies extensively on Stephanie K. Pell & Christopher Soghoian. See *supra* note 1.

34. The “Stingray” is actually just a trade name of one such device, which are known generically as International Mobile Subscriber Identity (IMSI)-catchers or cell site simulators.

35. Pell & Soghoian, *supra* note 1, at 11–12.

36. *Id.*

protected by weak encryption that is readily cracked.³⁷ Indeed, over the last decade or so, it has become possible for hobbyists to create rudimentary Stingrays for only a few hundred dollars apiece.³⁸

Nevertheless, the government engaged for decades in a concerted, coordinated, and determined effort to resist and oppose any official disclosure of information about police use of Stingray technology. This secrecy campaign has been wide-ranging, extending to state and local law enforcement. I describe the elements of this effort to resist disclosure presently.

The FBI has imposed secrecy obligations on state and local police by exploiting the Federal Communications Commission's (FCC) jurisdiction over the radio frequency spectrum. Manufacturers of Stingrays and similar devices that transmit signals must obtain equipment authorization from the FCC.³⁹ As a condition of these authorizations, which allowed sales only to police, the FCC directed that "state and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment."⁴⁰ The FBI used this condition to require state and local agencies to sign a nondisclosure agreement that forbade them from disclosing any information about the devices to the public.⁴¹ In addition, the federal government designated information about the devices as "Homeland Security Information" pursuant to 6 U.S.C. § 482(e), a statute that purports to preempt state and local laws that

37. *Id.* at 9–10.

38. *Id.* at 5, 47–54.

39. 47 U.S.C. § 301 (2018); 47 C.F.R. § 24.1 (2018); *see also* FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73100176 (Mar. 2, 2012), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=vPxvZeEaq4qhr7N5OMugqw%3D%3D&fcc_id=NK73100176 [<https://perma.cc/YAW4-TR9J>]; FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73166210 (Mar. 2, 2012), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=S02SFOCotzKlbdYCDPFIa%3D%3D&fcc_id=NK73166210 [<https://perma.cc/P779-HQQH>]; FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73092523 (Mar. 2, 2012), https://apps.fcc.gov/oetcf/eas/reports/Eas731GrantForm.cfm?mode=COPY&RequestTimeout=500&application_id=1qg4iWNE3Ijyqf%2F9UfNNSQ%3D%3D&fcc_id=NK73092523 [<https://perma.cc/EN6C-7X5N>].

40. *See* FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73100176, *supra* note 39; FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73166210, *supra* note 39; FCC, Grant of Equipment Authorization to Harris Corporation, FCC Identifier NK73092523, *supra* note 39.

41. *See* U.S. Dep't of Justice, Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations (June 29, 2012), <https://www.documentcloud.org/documents/1727748-nondisclosure-agreement.html> [<https://perma.cc/PYU7-2XHR>]; Adam Bates, *Stingray: A New Frontier in Police Surveillance*, 809 CATO INSTITUTE POLICY ANALYSIS 1 (2017), <https://www.cato.org/publications/policy-analysis/stingray-new-frontier-police-surveillance> [<https://perma.cc/BLA7-EYC6>].

might otherwise require disclosure.⁴²

Because of these nondisclosure agreements, states and localities have assiduously concealed the use of Stingray devices in criminal prosecutions. They have operated on the understanding that merely disclosing the existence and use of such a device would violate the federal nondisclosure requirement. In cases where it has appeared that the criminal prosecution may result in compelled disclosure of information about the device, prosecutors have sometimes dropped charges rather than permit disclosure.⁴³

Law enforcement has also resorted to other measures in an effort to conceal the use of a Stingray and, therefore, to avoid disclosure and challenges to the lawfulness of the technique. In many cases, it appears that when law enforcement obtains a court order or warrant meant to authorize the use of a Stingray, law enforcement omits any mention of the Stingray in the application or court order.⁴⁴ In some instances, the application and court order affirmatively misrepresent that police will obtain information from the telephone company when in fact police mean to bypass the telephone company by deploying a Stingray.⁴⁵ In such cases, the criminal defendant is unlikely to learn that a Stingray has been deployed—and therefore will be unable to challenge its use—unless there are other indicia of the Stingray's use and defense counsel is alert to the possibility.⁴⁶ This secrecy tactic may account for the small number (and recent vintage) of reported decisions assessing the legality of a Stingray's use.⁴⁷

42. Pell & Soghoian, *supra* note 1, at 38.

43. See, e.g., Ellen Nakashima, *FBI Clarifies Rules on Secretive Cellphone-Tracking Devices*, WASH. POST, May 14, 2015, https://www.washingtonpost.com/world/national-security/fbi-clarifies-rules-on-secretive-cellphone-tracking-devices/2015/05/14/655b4696-f914-11e4-a13c-193b1241d51a_story.html?utm_term=.047c571e87fc [<https://perma.cc/26NF-TABB>]; Robert Patrick, *Controversial Secret Phone Tracker Figured in Dropped St. Louis Case*, ST. LOUIS POST-DISPATCH (Apr. 19, 2015), http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html [<https://perma.cc/RXA7-MBTP>].

44. See, e.g., *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016); *id.* at 548 (Wood, C.J., dissenting); *United States v. Ellis*, 270 F. Supp. 3d 1134, 1158–59 (N.D. Cal. 2017); *United States v. Temple*, No. 15-CR-230-1 JAR (JMB), 2017 WL 7798109, at *33 (E.D. Mo. Oct. 6, 2017); *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747, 748–49 (S.D. Tex. 2012).

45. See, e.g., *Patrick*, 842 F.3d at 545; *id.* at 548 (Wood, C.J., dissenting); *Ellis*, 270 F. Supp. 3d at 1147.

46. Fourth Amend. Ctr., Nat'l Ass'n of Criminal Def. Lawyers, *Cell Site Simulators*, 2016 NAT'L ASS'N. CRIM. DEF. LAW. FOURTH AMEND. CTR. 1 https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-4-28_Cell-Site-Simulator-Primer_Final.pdf [<https://perma.cc/ZE3U-27CY>].

47. The first public judicial decision assessing the legal parameters governing law enforcement use of Stingrays was issued sua sponte by Magistrate Judge Brian Owsley in

Law enforcement agencies may also have concealed the use of Stingrays from criminal defendants and courts using a tactic known as “parallel construction.” This is the practice of conducting a second, parallel investigation designed to “discover” evidence that was previously identified using the secret technology.⁴⁸ When the government presents the evidence to the defendant or the court, it is only the second, “clean” investigation that is disclosed. This serves to avoid both exposure and adjudication of the novel technique in the context of a suppression motion. It appears that the FBI encouraged state and local law enforcement to engage in this tactic.⁴⁹

In 2015, in response to media reports about the sweeping federal secrecy mandate imposed upon state and local law enforcement, the FBI clarified its policy, explaining that states and localities were no longer prohibited from disclosing the mere *existence* of a Stingray and the fact of its use.⁵⁰ The FBI thus acknowledged that law enforcement could tell a criminal defendant that police had used the device. The FBI continues to maintain, however, that states and localities must resist, by all means necessary, compelled disclosure of information regarding the capabilities of such devices and the methods by which they are used—even requiring prosecutors to dismiss indictments.⁵¹

The FBI has explicitly invoked the anti-circumvention argument as its justification for these extraordinary efforts to conceal the use of Stingray devices by law enforcement at all levels of government. A 2014 affidavit from a senior FBI official contended, “information concerning this equipment, if

response to an *ex parte* application by the local U.S. Attorney’s Office seeking authorization to use the device. See *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 747. The next challenge was raised by a *pro se* criminal defendant who managed to discover the secret use of a Stingray device while imprisoned facing criminal charges. See *United States v. Rigmaiden*, No. 08-cr-814, 2013 WL 1932800 (D. Ariz. May 8, 2013); *infra* notes 232–236 and accompanying text.

48. See generally HUMAN RIGHTS WATCH, DARK SIDE: SECRET ORIGINS OF EVIDENCE IN U.S. CRIMINAL CASES (2018); Grayson, *supra* note 31; see also Fairfield & Luna, *supra* note 31, at 1042–43; Toomey & Kaufman, *supra* note 31, at 863–64.

49. See, e.g., Jenna McLaughlin, *FBI Told Cops To Recreate Evidence from Secret Cell-Phone Trackers*, INTERCEPT (May 5, 2016), <https://theintercept.com/2016/05/05/fbi-told-cops-to-recreate-evidence-from-secret-cell-phone-trackers/> [<https://perma.cc/X8ZU-8Y4K>]; John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS, Aug. 5, 2013, <http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805> [<https://perma.cc/NZ4K-ZZYL>]; HUMAN RIGHTS WATCH, *supra* note 48, at 18.

50. See DEP’T OF JUSTICE POLICY GUIDANCE, *Use of Cell-Site Simulator Technology* (Sept. 3, 2015), <https://www.justice.gov/opa/file/767321/download> [<https://perma.cc/A7JL-PRMA>] [hereinafter DOJ Guidance].

51. See e-mail from Christopher M. Allan, FBI, to Cyrus Farivar, ArsTechnica (May 15, 2015, 17:59), <https://www.documentcloud.org/documents/2082240-urgent-copy-of-stingray-statement.html> [<https://perma.cc/9BQK-8ERZ>].

made public, could easily impair the use of this investigative method.”⁵² The affidavit predicted that disclosure would permit the perpetrators in “criminal cases involving terrorism, kidnappings, murder, and other conspiracies” to evade detection and go unprosecuted. What the affidavit did not acknowledge, however, is that Stingray technology was by then available in the public domain and known to anyone who cared to investigate. It also did not grapple with the fact that there was common knowledge among criminals that police had various means to track the location of cell phones.⁵³

Public defender offices and civil liberties organizations, like the American Civil Liberties Union and the Electronic Privacy Information Center, have mounted a transparency campaign to try to force disclosure of information about police use of Stingrays. These groups and likeminded individuals have filed and litigated FOIA requests directed at both federal government⁵⁴ and state and local law enforcement.⁵⁵ These organizations have also sought to unseal records from cases in which it appears that the use of Stingrays may have been at issue.⁵⁶

Unsurprisingly, the government has opposed these efforts vigorously. In response to the FOIA lawsuits, the government has argued—among other things—that information about Stingrays may be withheld from the public pursuant to the FOIA exemption for law enforcement “techniques and

52. Morrison Affidavit, *supra* note 13, at 2; see Fred Clasen-Kelly, *Charlotte Police Investigators Secretly Track Cellphones*, CHARLOTTE OBSERVER (Oct. 18, 2014), <http://www.charlotteobserver.com/news/local/article9203591.html> [<https://perma.cc/2E8H-LVBW>].

53. See generally *The Wire* (HBO television broadcast 2002–2008).

54. See, e.g., Elec. Privacy Info. Ctr. v. FBI, 80 F. Supp. 3d 149 (D.D.C. 2015); ACLU of N. Cal. v. Dep’t of Justice, 70 F. Supp. 3d 1018 (N.D. Cal. 2014), *aff’d in part, rev’d in part*, 880 F.3d 473 (9th Cir. 2018); Soghoian v. U.S. Dep’t of Justice, 885 F. Supp. 2d 62 (D.D.C. 2012); ACLU of N. Cal. v. Dep’t of Justice, No. 13-CV-03127-MEJ, 2015 WL 3793496 (N.D. Cal. June 17, 2015), *modified upon reconsideration*, 2015 WL 393496 (N.D. Cal. June 17, 2015); ACLU of N. Cal. v. Dep’t of Justice, No. 12-cv-04008-MEJ, 2014 WL 4954121 (N.D. Cal. Sept. 30, 2014).

55. See *Hodai v. City of Tucson*, 365 P.3d 959 (Az. Ct. App. 2016) (accepting argument that disclosure of certain training manuals and other information regarding Stingrays could be withheld); *Martinez v. Cook Cty. State’s Attorney’s Office*, 103 N.E.3d 351 (Ill. App. Ct. 2018) (rejecting request for records about use of cell-site simulators because request was defective); *Rudenberg v. Chief Deputy Attorney Gen. of Del. Dep’t of Justice*, No. N16A-02-006(RRC), 2016 WL 7494900, at *4–10 (Del. Sup. Ct. Dec. 30, 2016) (determining extent to which court would consider “statement of interest” filed by the United States opposing disclosure of records about Stingrays pursuant to Delaware Freedom of Information Act), *subsequent determination* 2017 WL 7000854 (Del. Sup. Ct. Dec. 8, 2017); *N.Y. Civil Liberties Union v. Erie Cty. Sheriff’s Office*, No. 2014/000206, 2015 WL 1295966 (N.Y. Sup. Ct. Mar. 17, 2015) (ordering disclosure of various withheld records concerning cell-site simulators).

56. See *ACLU of N. Cal.*, 2014 WL 4954121, at *4–5.

procedures.”⁵⁷ The federal government has also sought to participate in litigation under *state* open records laws to enforce the confidentiality requirements it has imposed on state and local law enforcement.⁵⁸ A small number of courts have been skeptical of these arguments and rejected them.⁵⁹ But where courts have ordered disclosure, it has only been because a significant amount of information about Stingrays was already available in the public record and the government failed to demonstrate that disclosure of additional records would have revealed more granular details about the technique.⁶⁰

Because of these multi-pronged transparency efforts, we have learned more about the capabilities of these devices and the circumstances in which law enforcement believes it can use them. Still, some agencies continue to oppose disclosure of even the most basic information—like the cost of the devices and the number purchased—let alone information about the capabilities of the devices and guidelines governing their use.⁶¹

In parallel with the transparency campaign, advocates have undertaken efforts to establish legal standards about how this surveillance technology should be used. Before the concerted transparency effort around Stingrays kicked off, the rules governing their use were either shrouded in secrecy or nonexistent. It appears that many jurisdictions used Stingrays at will, without any prior judicial authorization,⁶² notwithstanding that a number of sources of law—including potentially state wiretap laws and Fourth Amendment limits—seem very likely to apply to most uses of the devices.

Now that Stingrays have begun to come out of the shadows, there has been movement toward legal oversight of the technology’s use. At least four state appellate courts have now held that a warrant based upon probable cause is required in order to deploy a Stingray.⁶³ Since 2015, at least five states have

57. See *supra* note 54 (collecting federal FOIA cases).

58. See, e.g., *Rudenberg*, 2016 WL 7494900; *N.Y. Civil Liberties Union*, 2015 WL 1295966.

59. See, e.g., *ACLU of N. Cal.*, 70 F. Supp. 3d 1018, *Rudenberg*, 2016 WL 7494900; *N.Y. Civil Liberties Union*, 2015 WL 1295966, at *11–13. But see *Sogboian*, 885 F. Supp. 2d at 74–75.

60. See *ACLU of N. Cal. v. Dep’t of Justice*, 880 F.3d 473 (9th Cir. 2018), *aff’g in relevant part* 70 F. Supp. 3d 1018 (N.D. Cal. 2014). But see *Sogboian*, 885 F. Supp. 2d at 74–75.

61. See, e.g., FOIL Request from N.Y. Civil Liberties Union to N.Y. Police Dep’t (Apr. 13, 2015), https://www.nyclu.org/sites/default/files/20150413_FOIL_request_NYPD_stingrays_web.pdf [<https://perma.cc/5NR3-QBZ4>]; Response to FOIL Request from N.Y. Police Dep’t to N.Y. Civil Liberties Union (Oct. 30, 2015), https://www.nyclu.org/sites/default/files/20151030_FOIL_response_NYPD_stingrays_web.pdf [<https://perma.cc/YQZ2-S3QM>].

62. See, e.g., *Stingrays*, N.Y. CIV. LIBERTIES UNION (last updated May 2016) <https://www.nyclu.org/en/Stingrays> [<https://perma.cc/F7HJ-N8D8>] (describing policies of various jurisdictions in New York).

63. See *Jones v. United States*, 168 A.3d 703, 711–17 (D.C. 2017) (finding that the use of a cell-site simulator to locate an individual is a search and requires a warrant based on probable

enacted laws requiring a warrant before a Stingray can be used to determine a person's location.⁶⁴ Moreover, at least four federal district courts have considered the Fourth Amendment limits on use of Stingrays.⁶⁵ Still, no federal appellate court has yet considered whether use of a Stingray even constitutes a "search" for purposes of the Fourth Amendment.⁶⁶ Meanwhile, the Department of Justice (DOJ) has made a voluntary policy change—perhaps in order to mitigate litigation risk and avoid binding precedent—that now requires the FBI to obtain a warrant to use a Stingray device unless one of two exceptions applies.⁶⁷ Other agencies have also now adopted internal policies.⁶⁸ But it is unclear how closely such policies are being followed, even within DOJ.⁶⁹

cause); *State v. Andrews*, 134 A.3d 324, 371–99 (Md. Ct. Spec. App. 2016) (finding the same); *Tracey v. Florida*, 152 So. 3d 504, 526 (Fla. 2014) (suppressing evidence obtained from a warrantless use of an IMSI catcher); *State v. Tate*, 357 Wis. 2d 172, 201 (Wis. 2014) (holding that a warrant was required to use cell-site simulator).

64. See CAL. PENAL CODE § 1546 (West 2015); 725 ILL. COMP. STAT. 137 (West 2016); UTAH CODE ANN. § 77-23c-102 (West 2016); VA. CODE ANN. § 19.2-70.3 (2016); WASH. REV. CODE § 9.73.260 (2015).

65. See *United States v. Ellis*, 270 F. Supp. 3d 1134, 1140 (N.D. Cal. 2017) (finding that the use of cell-site simulator is a search under the Fourth Amendment and requires probable cause); *United States v. Lambis*, 197 F. Supp. 3d 606, 610–11 (S.D.N.Y. 2016) (finding the same); *United States v. Temple*, No. 15-CR-230-1 JAR(JMB), 2017 WL 7798109, at *30–36 (E.D. Mo. Oct. 6, 2017) (finding that a court order founded upon probable cause was sufficient to authorize use of a cell-site simulator); *In re Application of the United States for an Order Relating to Telephones Used by Suppressed*, No. 15-M-0021, 2015 WL 6871289, at *3–4 (N.D. Ill. Nov. 9, 2015) (setting out Fourth Amendment requirements to minimize collection of innocent third party information when using cell-site simulator).

66. See *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (declining to determine whether use of a Stingray is a "search"); *id.* at 546 (Wood, J., dissenting) ("This is the first court of appeals case to discuss the use of a cell-site simulator, trade name 'Stingray.'").

67. See DOJ Guidance, *supra* note 50, at 3–5 (explaining that a warrant is required unless there are "exigent circumstances" or other unspecified "exceptional circumstances where the law does not require a warrant").

68. See *generally* COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., LAW ENFORCEMENT USE OF CELL-SITE SIMULATION TECHNOLOGIES: PRIVACY CONCERNS AND RECOMMENDATIONS 23–27 (Dec. 19, 2016), <https://assets.documentcloud.org/documents/3242927/The-FINAL-Bipartisan-Cell-Site-Simulator-Report.pdf> [<https://perma.cc/9DMH-CRDJ>] (describing and comparing the policies adopted by several federal agencies, including the Department of Homeland Security, the Internal Revenue Service, and the Treasury Inspector General for Tax Administration, as well as a number of local jurisdictions).

69. According to a discussion with a public defender at the Legal Aid Services of New York, the U.S. Marshals Service, working in cooperation with the New York Police Department (NYPD), deployed a Stingray without obtaining a warrant but instead on the basis of a court order that did not require probable cause. This alleged use of the Stingray by the Marshals Service, which is part of the DOJ, post-dated the DOJ's policy change.

B. THE MYSTERY OF MOBILE X-RAY VANS

Mobile x-ray vans present another archetypical example of innovative technology that police keep firmly under wraps. As with Stingrays, police have justified this secrecy as a measure to protect against circumvention. But, in practice, secrecy has ended up impeding any meaningful legislative, judicial, or public oversight.⁷⁰

According to the promotional material of the mobile x-ray van's manufacturer (which is freely available online), the vans operate by "directing a sweeping beam of x-rays at the object under examination, and then measuring and plotting the intensity of the scattered x-rays"⁷¹ The result is an image that clearly depicts organic material—drugs, explosives, and people—in silhouette.⁷² The promotional materials promise that police can use the vans on the streets even while in motion, at speeds up to six miles per hour, scanning cars and other objects that pass alongside and "provid[ing] a complete field of view of vehicles of all heights, including the tires."⁷³

The vans use the same x-ray backscatter technology that was at one point deployed in airports to conduct body scans. Those devices were criticized because of concerns about privacy: the devices' ability to see through clothes produced what some called "virtual strip searches."⁷⁴ There were also significant health concerns because the devices emit ionizing radiation.⁷⁵ The Transportation Security Administration ultimately removed the x-ray devices from airports in favor of devices that rely on "millimeter waves" and emit no

70. More than a decade ago, NYPD acquired this kind of mobile van equipped with x-ray technology. According to accounts by reporters embedded with the NYPD bomb squad, the vans have been used by NYPD since at least 2004. See RICHARD ESPOSITO & TED GERSTEIN, *BOMB SQUAD: A YEAR INSIDE THE NATION'S MOST EXCLUSIVE POLICE UNIT* (Hyperion Books 2017); Grabell, *supra* note 4. The NYPD Commissioner has acknowledged that NYPD has such vans. See Yoav Gonen & Shawn Cohen, *NYPD has super-secret X-ray vans*, N.Y. POST, Oct. 13, 2015, <http://nypost.com/2015/10/13/nypd-has-secret-x-ray-vans/> [<https://perma.cc/9K8C-W842>].

71. *Z Backscatter Technology Was Pioneered By AS&E*, AS&E, <http://as-e.com/resource-center/technology/z-backscatter/> [<https://perma.cc/7VTP-JTU9>].

72. *Id.*

73. *Mobile Z Backscatter Cargo and Vehicle Screening System*, AS&E, <https://www.rapiscan-ase.com/products/mobile/product/zbv> [<https://perma.cc/9996-UCXR>].

74. See *Competitive Enter. Inst. v. Dep't of Homeland Sec.*, No. 16-1135, 688 F. App'x 20, 2017 U.S. App. LEXIS 9324 (D.C. Cir. May 26, 2017); *Backgrounder on Body Scanners and "Virtual Strip Searches"*, ACLU, <https://www.aclu.org/aclu-backgrounder-body-scanners-and-virtual-strip-searches> [<https://perma.cc/RD47-EV8X>].

75. See Markham Heid, *You Asked: Are Airport Body Scanners Safe?*, TIME (Aug. 23, 2017), <http://time.com/4909615/airport-body-scanners-safe/> [<https://perma.cc/Y9YY-E7CM>].

radiation.⁷⁶

The vans raise similar health and privacy concerns. With respect to the health concerns, the manufacturer of the device contends that radiation doses are well below specified limits. Advertising material states that one scan of an object at a distance of five feet, conducted while the van is travelling at three miles per hour, delivers a radiation dose of 0.1 microsieverts, “equivalent to flying 2 minutes at altitude.”⁷⁷ But the exposure depends entirely on how the device is used by the police. If the device is closer to a target or if a particular location is repeatedly or continuously scanned, exposure levels would be higher.

The device also raises obvious privacy concerns. The specified purpose of the vans is to see inside vehicles and, perhaps, buildings, in order to identify objects not otherwise visible, including at least the silhouette of a person’s body beneath their clothes. Unlike airport scanners, x-ray vans can operate surreptitiously, without the subject’s knowledge or consent.

In many likely applications, the mobile x-ray vans will implicate the Fourth Amendment. For instance, the Fourth Amendment generally permits warrantless searches inside vehicles only if “probable cause exists to believe it contains contraband.”⁷⁸ In some limited circumstances, it may be permissible to conduct a suspicionless administrative search—for example, at the international border⁷⁹—but in ordinary policing, probable cause is required. The vans, however, are designed to be readily used to conduct indiscriminate searches. As the promotional material suggests, the van can scan vehicles on the streets as it drives by.⁸⁰ One can also easily imagine the van scanning all vehicles passing a particular traffic chokepoint (like, for example, the entrance to a bridge or tunnel).

There is little information about how broadly mobile x-ray vans are in use by police across the country, and what rules govern them. The New York Police Department (NYPD), which is one of the few departments known to have this technology, has disclosed neither what position it takes with respect to these Fourth Amendment concerns nor whether it uses the vans in ways that raise significant constitutional questions.

76. See Mike M. Ahlers, *TSA removes body scanners criticized as too revealing*, CNN (May 30, 2013), <http://www.cnn.com/2013/05/29/travel/tsa-backscatter/> [<https://perma.cc/3AP8-7B3Q>].

77. *ZBV Cargo and Vehicle X-ray Screening System*, AS&E, https://www.rapiscan-ase.com/uploads/documents/ZBV_Privacy_and_Safety_Assured.pdf [<https://perma.cc/Q255-TP97>].

78. *Pennsylvania v. Lebron*, 518 U.S. 938, 940 (1996).

79. See *United States v. Flores-Montano*, 541 U.S. 149, 155–56 (2004).

80. See *supra* note 73.

To the contrary, NYPD has made determined efforts to keep secret essentially all information about the vans, their capabilities, when and how they are used, and any policies or practices meant to address privacy and health concerns.⁸¹ There do not appear to be any reported criminal cases in which law enforcement has disclosed that an x-ray van was used in the course of an investigation. To the extent that police are using the devices to investigate, law enforcement appears to be either obscuring their role or declining to bring prosecutions where their use may become subject to discovery.

NYPD has also vigorously resisted efforts to pry loose information about the vans using the Freedom of Information laws (FOIL). ProPublica reporter Michael Grabell filed a Freedom of Information request with NYPD seeking information about the specifications of the vans, procurement costs, health and privacy policies, and information about how the police had used them in the past. NYPD refused to turn over any information at all.

Grabell sued to enforce the FOIL request. In response, NYPD argued that all of the information sought was exempt because it would disclose “techniques or procedures.”⁸² The NYPD’s submissions explicitly invoked the anti-circumvention rationale, focusing in particular on the notion that disclosure could allow terrorists to evade detection.⁸³ NYPD argued that disclosing even basic information about the cost or number of vans could allow terrorists to deduce information that would permit circumvention.⁸⁴ NYPD likewise refused to turn over any information about health, safety, and privacy because it could permit circumvention.⁸⁵

The trial court judge largely rejected these arguments and ordered significant disclosure after taking an unusually detailed, fact-intensive approach to the determination about whether disclosure could lead to circumvention.⁸⁶ In particular, the court found that NYPD could only withhold documents disclosing when and in what particular circumstances the vans may *not* be used.⁸⁷ The court reasoned that disclosure of such information “would extend a free pass from detection by the Van(s)” in such circumstances.⁸⁸ On the other hand, the court did order disclosure of information regarding (1) the locations where the vans had *previously* been used, (2) general policies, procedures, and

81. *See infra* notes 82–85.

82. *Grabell v. N.Y.C. Police Dep’t*, 996 N.Y.S.2d 893, 896 (Sup. Ct. 2014).

83. *Id.* at 210–15 (discussing Affidavit of Richard Daddario, NYPD Dep’t Comm. of Counterterrorism in Support of Answer). The author was among counsel for the petitioner in this case.

84. *Id.* at 212.

85. *Id.* at 213.

86. *Id.* at 210–16.

87. *Id.* at 212.

88. *Id.*

training materials (to the extent they did not disclose where vans could not be used), (3) information regarding the cost of the vans, (4) records describing the data retention/privacy policies governing the images taken by the vans, and (5) information regarding health and safety effects regarding their use.⁸⁹ With respect to all of these kinds of documents, the court found that NYPD had failed to make a detailed or persuasive showing that disclosure could actually create a substantial risk of circumvention.⁹⁰

On appeal, however, the appellate court was far less searching in its scrutiny of the anti-circumvention arguments presented by NYPD. The court agreed with NYPD's blanket argument that disclosing any information about "the strategies, operational tactics, uses and numbers of the vans would undermine their deterrent effect, hamper NYPD's counterterrorism operations, and increase the likelihood of another terrorist attack."⁹¹ In addition, disclosure of past deployments of the vans "would allow terrorists to infer the inverse, namely, locations and times when NYPD does not use them, and would permit a terrorist to conform his or her conduct accordingly."⁹² On this basis, the court allowed NYPD to withhold *all* information about the vans, except "tests or reports regarding the radiation dose or other health and safety effects," which amounted to a single three-page report.⁹³

In reaching this ruling, the appellate court was willing to defer to NYPD's high-level speculation about circumvention risk. For example, the court failed entirely to engage with the significant amount of public information already available about the vans, including images of the vans provided by the manufacturer, which would allow any would-be terrorist to identify whether a van is deployed in the immediate vicinity.⁹⁴

As a result of the decision, the public remains in the dark about when NYPD believes it can use the vans and how NYPD handles health and privacy concerns. It is entirely possible, for example, that NYPD uses the vans to perform random spot checks of city blocks. Or perhaps it routinely scans certain locations, regularly exposing pedestrians or an unwitting food vendor to significant doses of radiation. Perhaps it only uses the vans where it has probable cause to believe a vehicle contains contraband. Or maybe NYPD operates the vans without any suspicion at all, perhaps on the view that such searches fall within a controversial "special needs" exception to the Fourth

89. *Id.* at 205–06.

90. *Id.* at 210–16.

91. *Grabell v. N.Y.C. Police Dep't*, 139 A.D.3d 477, 478–79 (N.Y. App. Div. 2016).

92. *Id.* at 479.

93. *Id.*; Email from Susan Paulson, Senior Counsel New York City Law Department to John Langford and David Schulz, Counsel for Michael Grabell (Jan. 17, 2017) (on file with author).

94. *Grabell*, 139 A.D.3d at 478–79.

Amendment's warrant requirement because they are ostensibly aimed at protecting against terrorism, even if in practice they end up only turning up evidence of ordinary crime.⁹⁵

Not only is the public in the dark but also, importantly, regulation of the use of the vans has been left solely in the hands of the police. In the absence of basic information regarding the police's current practices, it has not been possible to mount court challenges or mobilize legislative efforts to rein in any potential abuses. Citizens and legislators are left to speculate about potential concerns, while the police can now point to a judicial opinion endorsing the notion that it would pose an unacceptable terrorism risk even to make public the non-binding internal guidelines, if any, that currently regulate the use of the vans. The anti-circumvention rationale thus continues not just to prevent transparency, but to postpone or frustrate any meaningful public deliberation or regulation even now, well over a decade after the technology was first acquired.⁹⁶

III. THE PROBLEM WITH SECRET LAW ENFORCEMENT TECHNOLOGIES

This Part examines the democratic costs that anti-circumvention secrecy imposes. In particular, it canvases how secrecy about police technology impairs the constitutional role of courts and legislatures, leading to a self-regulatory regime without meaningful checks on law enforcement. It also explores how anti-circumvention secrecy can upend the relationship between the public and police, to the detriment of both.

A. SECRECY IMPEDES THE ABILITY OF COURTS TO ADJUDICATE THE LEGAL LIMITS WITHIN WHICH NEW TECHNOLOGIES MAY BE USED

As we have already seen, many novel police technologies raise significant constitutional or statutory concerns. Police can use them in ways that press beyond established limits, or at least raise serious questions about their legality. Of course, regulation of the government's investigatory powers is a primary concern of the Constitution; the Bill of Rights contains multiple provisions that limit how the government may go about investigating individuals.⁹⁷ The statute books also contain detailed legal regimes meant to regulate investigative

95. *See, e.g.*, *MacWade v. Kelly*, 460 F.3d 260 (2d Cir. 2006) (upholding a suspicionless subway search program under the special needs doctrine on the theory that the programmatic purpose was to prevent terrorist attacks).

96. *See* Michael Grabell, *Split Decision on NYPD's X-ray Vans*, PROPUBLICA (May 10, 2016), <https://www.propublica.org/article/split-decision-on-nypds-x-ray-vans> [<https://perma.cc/75LR-5LFE>].

97. *See generally* U.S. CONST. amends. IV, V, VI.

and surveillance techniques.⁹⁸ Typically, we rely on the courts to authoritatively adjudicate the meaning of these constitutional and statutory provisions and the protections they do or do not offer in particular circumstances. Secrecy threatens to upend this check on law enforcement.

If techniques and capabilities are secret, then litigation is much more difficult, and perhaps impossible. Affirmative cases challenging such techniques are likely to fail because secrecy puts up threshold barriers to adjudication. For instance, plaintiffs will often be unable to establish standing to challenge a secret technique. The Supreme Court in *Clapper v. Amnesty International* held, with respect to a surveillance program, that plaintiffs lacked standing unless the “threatened injury [is] certainly impending.”⁹⁹ In particular, the Court required the plaintiffs to demonstrate that they were in fact targeted by the challenged surveillance program.¹⁰⁰ But the details of the program and its operations were a closely guarded secret, so the plaintiffs could not make that case.

Similar concerns thwart efforts to challenge other novel investigative methods—Stingrays, x-ray vans, and the like. Unless and until the police choose to reveal how these devices are used (and that certain individuals have been targeted), it will be difficult for any plaintiff to show that they have suffered an injury sufficient to establish standing. Put differently, the police can often guard against the prospect of affirmative litigation simply by keeping a tight lid on details about where, when, how, or against whom they are using these new technologies.¹⁰¹

Of course, constitutional and statutory adjudication may also arise in a defensive context, where a criminal defendant learns that police have used a certain method and the defendant chooses to contest it on a motion to suppress. But, as detailed already, the government has developed tactics, including filing opaque or misleading warrant applications, engaging in “parallel construction,” or simply dropping charges, that are designed to avoid

98. *See, e.g.*, Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (regulating wiretaps); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (regulating electronic communications while in transit and at rest, as well as regulation of pen register devices); Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 (1994)) (amending Electronic Communications Privacy Act); USA Patriot Act, tit. II, Pub. L. No. 107-56, 115 Stat. 272 (2001) (amending Electronic Communications Privacy Act and the Foreign Intelligence Surveillance Act); FISA Amendments Act, Pub. L. No. 110-261, 122 Stat. 2436 (2008); USA Freedom Act, Pub. L. No. 114-23, 129 Stat. 268 (2015) (limiting certain surveillance powers).

99. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 402 (2013).

100. *Id.* at 410–13.

101. *See* Manes, *supra* note 22, at 821–26 (examining various obstacles that secrecy poses to judicial oversight of programs).

adjudication by keeping criminal defendants in the dark that novel techniques have been used.¹⁰²

But even if law enforcement is not completely obscuring its reliance on novel techniques, it may provide defendants and courts with so few details about its techniques as to make constitutional adjudication nearly impossible. In a fairly recent decision of the Seventh Circuit Court of Appeals—the first federal appellate court to encounter the use of Stingrays—Judge Diane Wood elaborated on these problems in a lengthy dissent.¹⁰³ In that case, the government “appear[ed] to have purposefully concealed the Stingray’s use from the issuing magistrate, district court, and defense counsel.”¹⁰⁴ Indeed, the defendant had litigated his motion to suppress “based on the government’s representation that the officers tracked his location using information provided by the cell phone service provider.”¹⁰⁵ The government admitted the truth—that it had in fact used a Stingray and not records from the phone company—only after the defendant and supporting amici filed their briefs on appeal.¹⁰⁶

Even after admitting its use, however, the government refused to provide any details about “the way in which the Stingray . . . was configured” or “the extent of its surveillance capabilities.”¹⁰⁷ The government refused to say, for example, whether agents used the device solely to determine locations or whether they used it in an even more aggressive manner to “capture the e-mails, texts, contact lists, images, and other data.”¹⁰⁸ In the absence of this kind of information, Judge Wood contended that it was impossible for the court to adjudicate whether its use was constitutional or whether it was even authorized by the location-tracking warrant that the magistrate judge had issued in that case. As she lamented, “we must know how it works and how the government used it before we can judge whether it functions in a manner [consistent with] the location-gathering methods specified in the warrant” that was actually obtained.¹⁰⁹

102. Toomey & Kaufman, *supra* note 31; *see supra* notes 44–46 and accompanying text.

103. *United States v. Patrick*, 842 F.3d 540, 545–52 (7th Cir. 2016) (Wood, C.J., dissenting).

104. *Id.* at 546.

105. *United States v. Patrick*, No. 13-CR-234, 2016 U.S. Dist. LEXIS 59933, at *2 (E.D. Wisc. May 5, 2016).

106. *Patrick*, 842 F.3d at 546.

107. *Id.* at 547.

108. *Id.* (internal citations omitted).

109. *Id.* at 546.

Even in cases where the government concedes that it used a novel technology, it can avoid adjudication of constitutional questions by making strategic concessions. Thus, in at least one case, prosecutors conceded, solely for purposes of that particular case, that use of Stingrays was a “search” subject to the Fourth Amendment.¹¹⁰ By making that concession, the government avoided a judicial ruling on that central constitutional question.¹¹¹

Stingrays are but one example of how secrecy impedes judicial oversight. Twenty years after they came into use, courts are only beginning to grapple with Stingrays’ legality. The courts remain completely shut out of the picture with respect to many other novel technologies that have yet to see their moment in the sun. Secrecy, it turns out, does not just shield police technology from the public but also from the courts.

B. ANTI-CIRCUMVENTION ARGUMENTS MILITATE AGAINST
LEGISLATIVE ENACTMENTS THAT LIMIT HOW NEW TECHNOLOGIES
MAY BE USED

Litigation is only one means we have to regulate law enforcement’s use of technology. Legislatures at all levels of government have authority to enact laws imposing requirements upon the use of investigative techniques.¹¹² Secrecy, however, impedes this kind of democratic oversight and deliberation, as well. Indeed, the anti-circumvention argument specifically militates against the adoption of public rules governing novel technologies, because knowing these rules may create opportunities for circumvention.

Legislative efforts to regulate law enforcement capabilities are very difficult where the methods are secret because there will be no public pressure or electoral rewards for acting. Even if the existence of a technique is public (as with x-ray vans), the absence of information about how police use it will impede efforts to make the case for legislative action. Without vivid stories about how police use or misuse a technique, against whom, and for what purposes, it will be difficult or impossible to mobilize support for oversight.¹¹³ And without pressure from constituents, community groups, advocacy organizations, and the like, it is unlikely there will be a legislative response.

110. See *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 995–96 (D. Ariz. 2012); see generally *infra* notes 232–236 and accompanying text.

111. See *Rigmaiden*, 844 F. Supp. 2d at 996 n.6.

112. See, e.g., Electronic Privacy Communication Act, 2015 Stat. Cal. Ch. 651 (codified at Cal. Penal Code §§ 1546–1546.4 (2016)); Biometric Information Privacy Act, Ill. Pub. Acts 95-994 (codified at 740 Ill. Comp. Stat. § 14 (2008)).

113. See generally Deborah A. Stone, *Causal Stories and the Formation of Policy Agendas*, 104 POL. SCI. Q. 281 (1989).

The anti-circumvention rationale also discourages legislative oversight and regulation of novel law enforcement techniques for a more fundamental reason: the logic of anti-circumvention itself militates against having public rules or standards governing the use of a technology. The basic idea of anti-circumvention is that disclosing information about methods would give bad actors a roadmap to circumvent or evade them. But these same arguments militate against enacting public rules regarding how and when such techniques may be used. After all, to make rules governing a technology's use is both to confirm its existence and to disclose limits on its use. Anti-circumvention arguments, where accepted, therefore tend to be arguments not just against disclosure by law enforcement but against any kind of public, democratic regulation and control.

This troubling implication of the anti-circumvention argument is particularly acute with respect to contemporary and emerging electronic technologies. This is because the capabilities of a technology (and, therefore, potential vulnerabilities) can be defined either by technological limits or legal limits on its use.¹¹⁴ Whether a Stingray can intercept the content of text messages is as much a question of the technical capabilities of a particular device as it is a question about whether and in what circumstances the law allows police to use it in this way. Put differently, from the perspective of the hypothetical criminal seeking to circumvent the Stingray, knowing that the Stingray cannot technically intercept the content of text messages provides similar prospects for evasion as knowing that the Stingray cannot be used to intercept text messages unless the police already have probable cause and have obtained a warrant covering a particular cell phone. Thus, when it comes to technology, anti-circumvention arguments often stray from a concern to avoid disclosure of technical information into a concern to avoid disclosure of legal and policy limits.¹¹⁵

In practice, secrecy has indeed resulted in legislative action being avoided, misdirected, or delayed. With respect to Stingray devices, former prosecutor Stephanie Pell and technologist Christopher Soghoian have documented that legislatures at every level have for decades refused to engage seriously the possibility of regulating the manner in which law enforcement used these devices.¹¹⁶ Instead, lawmakers enacted laws limiting the sale of Stingrays in a futile effort to prevent bad actors from obtaining the same capabilities to surveil cell phone networks as police.¹¹⁷ Legislatures declined to act even

114. *See generally* LAWRENCE LESSIG, CODE 1–9 (2d ed. 2006) (arguing famously that “code is law”).

115. *See supra* notes 48–49 and accompanying text.

116. Pell & Soghoian, *supra* note 1, at 2–8.

117. *Id.* at 3–4 & nn.9–10.

though nearly all of the “sensitive” capabilities they aimed to protect were in fact already a matter of public record, well-known among technologists and privacy specialists and also, presumably, among the kind of sophisticated criminals who would take countermeasures to circumvent the devices.¹¹⁸ It is only now—after Stingrays received significant media attention, after a sustained public education campaign by advocacy organizations, and after a multi-pronged litigation campaign—that legislatures are beginning to pay attention and consider regulating these devices.¹¹⁹ Efforts to regulate other relatively novel law enforcement techniques have likewise struggled, in large part due to the secrecy under which they currently operate.¹²⁰

C. NEW TECHNOLOGIES AND OLD LAWS PRODUCE UNACCOUNTABLE SELF-REGULATION BY POLICE

Secrecy about police technology also exacerbates a regulatory problem that is familiar within studies of law and technology: old laws, drafted in a particular historical and technological context, tend to be a poor fit with new technologies whose capabilities and operation simply could not have been envisioned by earlier legislators. New technologies are thus often misregulated, subject to rules that are too strict, too lenient, or simply ill-formed.

118. *Id.* at 6–8.

119. Tim Cushing, *House Oversight Committee Calls for Stingray Device Legislation*, TECHDIRT (Dec. 22, 2016), <https://www.techdirt.com/articles/20161219/15052936308/house-oversight-committee-calls-stingray-device-legislation.shtml> [<https://perma.cc/K9JE-X7UG>]; COMM’N. ON OVERSIGHT AND GOV’T REFORM, 114TH CONG., LAW ENFORCEMENT USE OF CELL-SITE SIMULATION TECHNOLOGIES: PRIVACY CONCERNS AND RECOMMENDATIONS (2016), <https://assets.documentcloud.org/documents/3242927/The-FINAL-Bipartisan-Cell-Site-Simulator-Report.pdf> [<https://perma.cc/JK9P-8G89>].

120. For example, facial recognition technology is coming into widespread use by police, yet there are extraordinarily few states with laws governing their use. *See* Garvie et al., *supra* note 5, at 35–36. To take another example, automated license plate reader (ALPR) technology has been available since the 1990’s and was in very widespread use by 2012, at which point 71% of law enforcement agencies reported using the devices. *See* Jeremy Hsu, *70 Percent of U.S. Police Departments Use License Plate Readers*, IEEE SPECTRUM (July 8, 2014), <https://spectrum.ieee.org/cars-that-think/transportation/sensors/privacy-concerns-grow-as-us-police-departments-turn-to-license-plate-readers> [<https://perma.cc/YS3C-H6WH>]. Nevertheless, only two states had enacted any kind of ALPR legislation by 2012. *See* CAL. VEH. CODE § 2413 (West 2011); ME. REV. STAT. ANN. tit. 29-A § 2117-A (2009). Even today, when the vast majority of police departments have adopted the technology—and use it daily to collect massive quantities of data about the location of private vehicles—only 16 states have any legislation relating to the use of ALPRs or the retention and sharing of data collected with ALPRs. *See* NAT’L CONFERENCE OF STATE LEGISLATURES, *Automated License Plate Readers: State Statutes* (Mar. 15, 2019), <http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx> [<https://perma.cc/H6GL-P22P>].

In the context of law enforcement, however, this problem of regulatory lag has a different valence: secrecy prevents (or at least delays) the development of rules governing novel technologies. As we have seen, the parts of government that typically set rules for policing—the courts and legislatures—simply cannot function properly when the techniques themselves are shrouded in secrecy.¹²¹ Secrecy thus impedes the ability of courts to adapt existing constitutional and statutory frameworks to new technologies, and it prevents legislatures from enacting new legislation. Secrecy, in other words, fosters a system of de facto self-regulation in which police agencies decide for themselves whether and how existing laws apply.

This problem of regulating novel police technologies is a special case of the broader problem—much examined in the literature—about the interaction between new technologies and old laws. Much of the literature centers on the relative merits of technology-neutral laws, which are intended to lay down principles that can be applied no matter how technology evolves, versus technology-specific laws, which govern only a particular kind of technology but do it well, and leave it for future legislators to confront whatever the future might bring.¹²²

With respect to novel police capabilities, there can be legislation enacted to address particular forms of technology,¹²³ as well as general technology-neutral laws governing police—most prominently, the Fourth Amendment to the Constitution.¹²⁴ Unfortunately, the anti-circumvention justification for secrecy upends both modes of regulation.

Regulation of technology according to technology-neutral laws relies fundamentally on the existence of an institution that can make the judgments necessary to adapt the broad, neutral language of the law to a particular, novel circumstance. In many cases, that institution is the courts. The Fourth Amendment is a classic example: it has largely been up to the courts to

121. See *supra* Sections III.A–B.

122. See generally Brad A. Greenberg, *Rethinking Technology Neutrality*, 100 MINN. L. REV. 1495 (2016); Paul Ohm, *The Argument Against Technology Neutral Surveillance Laws*, 88 TEX. L. REV. 1685, 1687–700 (2010); Lyria B. Moses, *Recurring Dilemmas: The Law's Race to Keep Up With Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239 (2007).

123. For example, new law enforcement tools to hack into servers or plant malware may run up against existing technology-specific laws governing access to stored communications on a “remote computing service” or “electronic communication service.” See Stored Communications Act of 1996, 28 U.S.C. §§ 2701–2712 (1996).

124. See Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1015–17 (2010) (describing the “deeply entrenched judicial consensus . . . that technology neutrality is the proper approach to the Fourth Amendment”); see also Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 748 (2005).

elaborate whether and how it regulates novel law enforcement methods.¹²⁵ Other institutions can play this updating role, too. For example, the Federal Trade Commission (FTC), an administrative body, shares authority with the courts to adapt technology-neutral protections against “unfair or deceptive acts or practices” to suit contemporary needs.¹²⁶ Specifically, the FTC can bring administrative proceedings to enforce these consumer protection standards and, ultimately, sue in court to enforce its determinations. The FTC, with the cooperation of the courts, has used this mechanism to enforce basic privacy and consumer fairness measures online, adapting the century-old provisions of the Federal Trade Commission Act of 1914 to the Internet.¹²⁷

Secrecy regarding novel law enforcement techniques upends this model of technology-neutral regulation. If law enforcement is permitted to keep secret information about the capabilities it has and how they use them, outside institutions that might otherwise be able to determine how old, neutral laws should apply cannot do so. We have already seen an instance of this in the examples of Stingrays and mobile x-ray vans: the courts have been unable to elaborate how Fourth Amendment standards apply to these technologies precisely because of the government’s furtiveness, which, in turn, has been justified by supposed anti-circumvention concerns.¹²⁸

The interplay between secrecy and legal regulation is different and perhaps more straightforward when it comes to technology-specific regulation. Secrecy simply delays the adoption of laws that specifically regulate new technologies. As already described in the prior Section, where the details of a technology are secret, they do not attract legislative interest. To the contrary, the anti-circumvention justification for secrecy is itself an argument against enactment

125. Perhaps the most famous example of the courts playing catch-up with technology in the Fourth Amendment context is the Supreme Court’s treatment of wiretapping. *See* *Olmstead v. United States*, 277 U.S. 438, 466 (1928) (holding that telephone wiretaps did not implicate the Fourth Amendment because they did not involve a physical trespass); *id.* at 471 (Brandeis, J., dissenting); *Katz v. United States*, 389 U.S. 347, 353–56 (1967) (overruling *Olmstead* and holding wiretapping is a “search” within the meaning of the Fourth Amendment and requires prior judicial authorization); *see also* *United States v. Jones*, 565 U.S. 400 (2012) (providing a more recent example of the Court’s treatment of GPS tracking devices); *Riley v. California*, 573 U.S. 373 (2014) (regarding cell phones); *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (regarding historical cell-site location information).

126. Federal Trade Commission Act of 1914, ch. 311, § 5, 38 Stat. 717 (codified as amended at 15 U.S.C. § 45 (2018)).

127. *Id.*; *see generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 2015 GEO. WASH. L. REV. 2230 (2015); Chris Jay Hoofnagle, *FTC Regulation of Cybersecurity and Surveillance*, in *THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW* (David Gray & Stephen E. Henderson, eds., 2017).

128. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 546 (7th Cir. 2016) (Wood, C.J., dissenting).

of technology-specific regulation because any such regulation would necessarily reveal something about technology and the limitations placed upon its use.

Secrecy thus cuts external institutions out of the loop, hampering the ability of courts and legislatures to update old laws or enact new ones. In fact, secrecy leaves only one institution in a position to determine how old laws should apply to new technologies—law enforcement itself. Rather than having an *outside* institution determine how laws should be adapted, secrecy leads inexorably to a self-regulatory model of policing. Law enforcement agencies themselves decide what limits they must respect. The examples of x-ray vans and Stingrays provided in Part II illustrate the phenomenon: in each case, the agency itself has developed the rules governing their use. In the case of x-ray vans, those rules remain secret and entirely uncertain.¹²⁹ In the case of Stingrays, the rules were secret until very recently, when the DOJ, Department of Homeland Security, IRS, and other federal agencies each issued separate guidance about when warrants are required before an investigator can use a Stingray.¹³⁰

One of the principal consequences of this self-regulatory model is that law enforcement will usually opt for the most permissive application of existing laws. Indeed, with respect to Stingrays, recent investigative efforts have revealed that some state and local departments had no policy documents at all regarding when they could use Stingrays.¹³¹ In other instances, the police had misled the public about how it was applying existing laws and told reporters that Stingrays were only used with prior judicial authorization, when in fact the police agency in question only obtained a court order in one out of forty-seven deployments of the Stingray during a three-and-a-half-year period.¹³² In short, the consequence of secrecy is under-regulation.¹³³

Secrecy impedes the process of law catching up with new technology in one additional and very important way: it can create an entrenchment problem. Because the anti-circumvention justification for secrecy pushes courts,

129. *See supra* Section II.B.

130. *See* COMM'N. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., *Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations* (2016), <https://assets.documentcloud.org/documents/3242927/The-FINAL-Bipartisan-Cell-Site-Simulator-Report.pdf> [<https://perma.cc/DY8H-RWWC>].

131. *See* *Stingrays*, N.Y. CIV. LIBERTIES UNION (last updated May 2016) <https://www.nyclu.org/Stingrays> [<https://perma.cc/UBC2-NT8F>] (describing findings with respect to New York State Police).

132. *See id.* (describing findings with respect to Erie County Sheriff's Department).

133. The Georgetown Center for Privacy and Technology has documented a similar pattern with respect to police self-regulation of facial recognition technology. *See* Garvie et al., *supra* note 5, at 36–40.

legislatures, and other institutions to the sidelines, it leaves the field open for law enforcement to establish and entrench new practices and policy baselines. Police agencies can roll out a new technology, determine the most advantageous ways to use it, and develop protocols regarding such use in secret. These practices will enjoy the advantages of incumbency; they will become the status quo. By the time the coordinate branches—and the public—enter the field to scrutinize the technology, any departures from the status quo will meet powerful opposition. The law enforcement establishment will be accustomed to acting with a certain freedom. It will presumably be armed with anecdotes or data about the benefits to crime detection and prevention that come from relatively unfettered use of the technology. Correspondingly, there will be anecdotes or data about the threat to public safety that would result from putting additional limits on its use. In the face of these temporal, evidentiary, and rhetorical advantages enjoyed by law enforcement, advocates for greater judicial or legislative regulation of a technology are left trying to roll the proverbial boulder back up the hill. In short, secrecy about novel technologies not only gives law enforcement the preeminent and primary role in regulating that technology but also gives it considerable political and legal power to entrench its preferred regulatory frame in perpetuity.

D. SECRET TECHNOLOGIES RECONFIGURE THE RELATIONSHIP
BETWEEN CITIZEN AND STATE

Allowing law enforcement to keep its capabilities and methods secret may also pose a more fundamental challenge. In a liberal democracy such as ours, we are committed to the proposition that individuals enjoy a sphere of freedom from intrusion by the government. One important way that we protect this conception of the relationship between government and individual is to allow the public to know what power the state potentially wields. This means allowing the public to know what investigative tools the government has at its disposal and the limits on their use.

An illustration helps make the point: imagine that the government develops hacking software that permits it to obtain easy access in bulk to all of the microphone and recording capabilities of every smartphone. The government has effectively transformed every smartphone into a listening device. This technology would raise profound privacy concerns. Now imagine that the public did not know the rules that governed when the government could switch the technology on.¹³⁴ The threat to civil liberties would be much

134. While it may seem obvious that surreptitiously turning on a recording device would require a warrant founded upon probable cause, one can at least imagine creative arguments that would permit warrantless use of such a device. For example, an enterprising law

worse, and not simply because the new tool might be misused and abused by rogue officials, but also because citizens would be left in a fundamentally vulnerable position, at the mercy of the state's secret decision about how broadly it can cast its net. The situation would be worse still if the very *existence* of this surveillance capability were a secret. In that case, citizens would not even know that the government could exercise these surveillance powers and would have no inkling that they might want to take democratic action to rein in those powers.

In this way, secrets about law enforcement techniques tend to invert the democratic relationship between the individual and government: the government's power expands in ways that are invisible to the citizenry and not subject to its control. Transparency is a fundamental safeguard that protects individuals against such encroachments by the state.¹³⁵

At the same time, surveillance technology, by its nature, expands the stock of information that the government may obtain about citizens. Thus, while the public is in the dark about the scope of the police's investigatory power, the government has access to ever more information about individuals. History suggests that this information asymmetry can readily breed abuse, particularly in the absence of strong external checks.

This type of threat to individual liberties was illustrated most vividly in the United States by the Hoover-era FBI, and its secretive "black bag jobs" and other surveillance. For decades following the Second World War, the FBI engaged in illegal and secret operations involving breaking-and-entering, wiretaps, opening postal mail, and other invasive methods.¹³⁶ These operations often targeted political dissenters, activists, protestors, and political leaders.¹³⁷ Such activities proliferated precisely because Hoover's FBI was able to keep them secret.¹³⁸

enforcement agency might argue that individuals enjoy no expectations of privacy with respect to conversations they have on the street in public, and so no warrant is required in such spaces. *See* 18 U.S.C. § 2510(2) (2018) (defining "oral communication" for purposes of the federal prohibition on warrantless interception to). One may also imagine law enforcement invoking various "special needs" exemptions to the warrant and probable cause requirement. In any case, the point is not to argue that any of these legal theories is plausible, only to show that if the technology and the rules are secret there is significant cause for alarm.

135. *See* Manes, *supra* note 22, at 814–17.

136. *See* ATHAN G. THEOHARIS & JOHN STUART COX, *THE BOSS: J. EDGAR HOOVER AND THE GREAT AMERICAN INQUISITION* 7–15 (1988); TIM WEINER, *ENEMIES: A HISTORY OF THE FBI* 191–201, 278–79 (2012).

137. *See* THEOHARIS & COX, *supra* note 136, at 14–15; WEINER, *supra* note 136, at 195–201.

138. *See* THEOHARIS & COX, *supra* note 136, at 361–78; Smith, *supra* note 28, at 245–46.

Indeed, as Judge Stephen Wm. Smith has shown in a fascinating recent article, the current legal doctrines that give the police the right to keep their techniques secret—i.e., the FOIA exemptions and the evidentiary privilege for law enforcement techniques that this Article focuses on—actually trace their roots directly back to Hoover himself.¹³⁹ Hoover dreamed up the idea of legal protection for the secrecy of techniques in the wake of *United States v. Coplon*, a high-profile prosecution of an alleged communist spy.¹⁴⁰ That case resulted in two calamities for the FBI. First, the court ordered an unprecedented disclosure of the FBI's illegal wiretapping operations, which showed them to have been approved at the highest levels of the FBI.¹⁴¹ Second, on appeal, the Second Circuit suppressed the illegally obtained evidence and reversed the conviction.¹⁴² As Judge Smith recounts, the lesson Hoover learned from the embarrassing episode was not to stop his agents from breaking the law, but to do a better job of keeping it secret—whether that meant hiding any paper trail or, alternatively, obtaining legal shields against disclosure.¹⁴³ Six years after the botched *Coplon* prosecution, Hoover publicly advocated for the latter course, publishing an article in the *Syracuse Law Review* proposing that law enforcement should have an evidentiary privilege shielding its techniques from discovery.¹⁴⁴ It was the first time that anybody proposed this kind of privilege.¹⁴⁵ And the idea was plainly motivated by the embarrassment and damage that Hoover's FBI had suffered when its illegal conduct was revealed in the *Coplon* case.¹⁴⁶

Of course, there may still be *good* reasons to have protection for secret law enforcement techniques, even if such protection has its origins in a desire to perpetuate a system in which law enforcement enjoyed unchecked and oft-abused powers.¹⁴⁷ But the capacity for this particular kind of secrecy to shield wrongdoing and expand the power of the state unchecked has been evident from the start.

The extent to which secrecy is currently shielding illegality or abuses from coming to light is unclear. There is evidence, however, that secrecy is enabling aggressive and troubling uses of novel technologies. For example, there have

139. Smith, *supra* note 28, at 242–46; *see also* John Edgar Hoover, *The Confidential Nature of FBI Reports*, 8 SYRACUSE L. REV. 2 (1956).

140. *Id.* at 9–11; *United States v. Coplon*, 185 F.2d 629 (2d Cir. 1950).

141. *See* Smith, *supra* note 28, at 234, 237–40.

142. *Coplon*, 185 F.2d at 640.

143. *See* Smith, *supra* note 28, at 242–46.

144. *See* THEOHARIS & COX, *supra* note 136.

145. *See* Smith, *supra* note 28, at 234.

146. *Id.*

147. *See infra* Part IV (examining in detail the arguments for keeping law enforcement techniques secret).

been alarming revelations about the scope of government surveillance powers exercised not just by intelligence agencies like the NSA, but also by federal law enforcement. Prime among these examples is the Drug Enforcement Administration's (DEA) Hemisphere program, in which the DEA compiled a truly massive database of telephone records that logged billions of domestic and international calling records every day.¹⁴⁸ The database apparently includes not just information about who has called whom, but also the locations of callers—something that was omitted even from the NSA's similar domestic call database, made famous by Edward Snowden's disclosures to the press.¹⁴⁹ The DEA's efforts to hide this program, which have included the aggressive use of “parallel construction,” suggest that it, like Hoover's FBI, may be just as concerned with evading public scrutiny and legal oversight as it is with protecting the efficacy of a law enforcement technique.¹⁵⁰

Moreover, because contemporary surveillance tools are often able to sweep up massive quantities of data over extended periods, the threat to individual liberties does not necessarily abate as time passes and technologies become known. To the contrary, as more and more data is stored and made searchable for law enforcement, law enforcement's power to reach back and investigate a particular person grows apace.¹⁵¹ For example, the swift proliferation of body cameras among police departments has been accompanied by the growth of online services that provide storage and hosting of the recorded videos. These databases store millions of hours of footage taken by on-duty police officers across the nation.¹⁵² As voice-to-text and facial recognition algorithms improve, these video databases are likely to become readily searchable.¹⁵³ In a few years, law enforcement may be able to reach back in time and pull out from massive archives of footage anything that matches a

148. See Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES, Sept. 1, 2013 (describing the Drug Enforcement Administration's “Hemisphere” program).

149. See *id.*; *ACLU v. Clapper*, 785 F.3d 787, 794 (2d Cir. 2015) (NSA data included “call-routing information” but not “cell site locational information, which provides a more precise indication of a caller's location than call-routing information does”).

150. See *Hemisphere: Law Enforcement's Secret Call Records Deal with AT&T*, ELEC. FRONTIER FOUND., <https://www.eff.org/cases/hemisphere> [<https://perma.cc/P8ZW-67EA>].

151. See *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (discussing this phenomenon with respect to historical cell-site location data).

152. See, e.g., Beryl Lipton, *Shifting from Tasers to AI, Axon wants to use terabytes of data to automate police records and redactions*, MUCKROCK (Feb. 12, 2019), <https://www.muckrock.com/news/archives/2019/feb/12/algorithms-ai-task-force/> [<https://perma.cc/9YXM-JCF4>]; Josh Sanburn, *Storing Body Cam Data is the Next Big Challenge for Police*, TIME (Jan. 25, 2016), <http://time.com/4180889/police-body-cameras-viewu-taser/> [<https://perma.cc/3AT9-ZU2F>].

153. See Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1594 (2017).

particular individual.¹⁵⁴ As Professor Elizabeth Joh has written, this kind of “big data” policing could also allow for automated “identification of large numbers of suspicious activities and people by sifting through large quantities of digitized data.”¹⁵⁵ Such capabilities could easily transform the power of government to engage in both criminal law enforcement and non-criminal regulation through, for example, the child protection system, immigration enforcement, welfare and social benefits agencies, and other regimes.¹⁵⁶

Put simply, a world in which police have such vast investigatory capacities would radically reorient the nature of law enforcement and its power to investigate and regulate individuals.¹⁵⁷ If police adopt such technologies in secret, citizens lose a powerful check against abuses and largely surrender the opportunity for meaningful public accountability that lies at the heart of our democratic constitutionalism.

E. SECRECY IMPOSES COSTS ON LAW ENFORCEMENT TOO

Thus far, this Article has focused on the normative costs that secrecy imposes from the point of view of citizens and democratic checks and balances. But there is also reason to believe that secrecy is a two-edged sword for law enforcement. The premise of the anti-circumvention argument is that police must keep secrets in order to preserve their investigative advantage over criminals. But secrecy also imposes costs on the law enforcement agencies in terms of public confidence, public input, and open exchanges of best practices.

For the reasons explored in the prior subsection, secrecy about intrusive police technologies will breed distrust among the public. Citizens who are not otherwise inclined to presume the police’s good intentions are likely to regard secrecy with suspicion, cutting against the efforts of police departments to establish cooperative relationships with the communities they serve. Indeed, a major strand of the contemporary discussion around policing focuses on the

154. See Zak Doffman, *Facial Recognition is Coming to Police Body-Worn Cameras in 2019*, FORBES (Jan. 10, 2019), <https://www.forbes.com/sites/zakdoffman/2019/01/10/body-worn-2-0-how-iot-facial-recognition-is-set-to-change-frontline-policing/#4820caf01ff3> [<https://perma.cc/5GWW-LYHR>] (discussing the future of real time and systematized facial recognition).

155. Elizabeth Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL’Y REV. 15, 19 (2016).

156. See generally Jennifer Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327 (2014) (examining the broad powers law enforcement has to regulate people using watchlists and other means that impair an individual’s freedom short of incarceration).

157. See generally Christina M. Mulligan, *Perfect Enforcement of Law: When To Limit and When To Use Technology*, 14 RICH. J.L. & TECH. 13 (2008) (examining the consequences and normative challenges posed by technology that could permit perfect surveillance or perfect detection of criminal violations).

idea of building trust between law enforcement and citizens.¹⁵⁸ The literature suggests that police-community relations improve when the public regards policing as legitimate.¹⁵⁹ Transparency is one piece of establishing such legitimacy, as part of a broader focus on establishing perceptions of procedural justice in the community.¹⁶⁰

Transparency also benefits police in another way: it allows the police the benefit of input and advice from experts and laypeople alike. Where technologies or the rules that govern them are secret, police are limited to relying on whatever expertise they have in-house or, more likely, the recommendations of the outside vendor who sold them the technology.¹⁶¹ Secrecy makes it difficult or impossible for police to open up their practices to constructive input from experts, other law enforcement agencies, or the public itself. This breeds suboptimal practices. Perhaps police will underutilize a technology because police do not realize all of its potential applications. Perhaps police will overuse a technology or use it too haphazardly because officers have not been presented with more efficient (or more legally defensible) means of deploying it. If techniques are public, law enforcement may even be motivated to find more creative—and perhaps more effective—approaches to its investigations that don't rely on secret methods.

In these ways, secrecy throws up obstacles to law enforcement, potentially frustrating efforts to improve police-community relations and impeding the flow of advice, experimentation, and expertise about how to use novel technologies. In some cases, at least, it seems that law enforcement may determine that it is in its own best interests not to forego the potential benefits of transparency in order to try to prevent circumvention at the margins.

IV. THE LOGIC OF ANTI-CIRCUMVENTION SECRECY

The previous Part argued that secrecy justified on anti-circumvention grounds raises serious normative and policy concerns. This Part takes the anti-circumvention rationale seriously on its own terms in order to understand its strengths and its limits. It begins by describing the logic of anti-circumvention:

158. See, e.g., LORAIN MAZEROLLE ET AL., LEGITIMACY IN POLICING 4–5 (U.S. Dept. of Justice, Office of Community Oriented Policing Services, Legitimacy in Policing No. 10 2013); POLICE EXECUTIVE RESEARCH FORUM, OPERATIONAL STRATEGIES TO BUILD POLICE-COMMUNITY TRUST AND REDUCE CRIME IN MINORITY COMMUNITIES: THE MINNEAPOLIS CEDAR-RIVERSIDE EXPLORATORY POLICING STUDY 1–3, 10–12 (2017).

159. See generally Tom Tyler, *Procedural Justice and Policing: A Rush to Judgment?*, 13 ANN. REV. L. & SOC. SCI. 29 (2017); Tracy Meares, *The Path Forward: Improving the Dynamics of Community-Police Relationships to Achieve Effective Law Enforcement Policies*, 117 COLUM. L. REV. 1355, 1360 (2017).

160. See Meares, *supra* note 159, at 1362–63.

161. See Crump, *supra* note 12; Joh, *supra* note 12.

what empirical and analytic claims the anti-circumvention argument for secrecy relies on. It then proceeds to unpack the normative assumptions built into the anti-circumvention argument.

The basic anti-circumvention argument for secrecy is deceptively simple and compelling. The logic proceeds as follows: If law enforcement discloses information about its capabilities (including how they are used or the rules governing their use), those disclosures will increase the stock of information available to the general public, including potential criminals. People planning crimes can use such information in order to devise ways to evade law enforcement's capabilities or to navigate around their limits. The underlying normative premise is that this kind of evasion of law enforcement is always a bad thing because it makes it more difficult to prevent or solve crimes.

This logic was vividly dramatized in one particular scene of Martin Scorsese's classic mobster film *Casino*.¹⁶² The film centers on Sam "Ace" Rothstein (played by Robert DeNiro), who has been tapped by the mob to oversee the Tangiers Casino in Las Vegas. The mob has sent in an enforcer, Nicky Santoro (played by Joe Pesci), to make sure that the casino's profits are being properly skimmed. The FBI is hot on their trail, wiretapping Ace and Nicky's calls. It is getting hard for them to communicate privately.

Ace describes the predicament in an extended voice-over: "[J]ust getting a call from Nicky wasn't easy anymore. Even the [code words] didn't work anymore. So, we figured out another act."¹⁶³

Ace continues narrating, describing his intimate knowledge of the FBI's wiretap minimization rules: "You see, if a phone's tapped, the Feds can only listen in on the stuff involving crimes. So on routine calls, they have to click off after a few minutes."¹⁶⁴

While Ace is delivering this voice-over, the audience watches Ace and Nicky's wives chat on the phone, planning a supposed shopping trip. Ace and Nicky are waiting impatiently next to them. The shot cuts to a bored FBI agent at a desk with a tape recorder, glancing at his watch. A few beats later, the agent looks at his watch again and clicks off the recording device. Immediately, Ace and Nicky grab the phones from their wives and quickly set a time to meet in the desert outside town. They hand the phones back to their wives who pick up their inane conversation. The FBI agent clicks back on to the line unaware that he just missed his targets.¹⁶⁵

162. *CASINO* (Universal Pictures 1995), at 1:52:40.

163. *Id.*

164. *Id.*

165. *Id.*

The scene illustrates exactly what the anti-circumvention rationale is getting at. Ace and Nicky are able to evade law enforcement because they know details about how the FBI carries out its wiretaps; indeed, in this case it is the very laws that govern wiretaps that permit circumvention.¹⁶⁶ Because they know that the FBI has to stop wiretapping routine calls after some time, the FBI misses an important lead and the mobsters are able to meet and make plans undetected. The anti-circumvention argument says that the limits on government wiretaps should have been kept secret in order to prevent Ace and Nicky from evading the FBI.

The scene also illustrates the limitations of the anti-circumvention argument. In particular, it shows how the argument depends crucially on a number of empirical and normative claims.

First, the anti-circumvention argument depends essentially on the idea that there is a sophisticated criminal who gathers technical details about law enforcement's methods and then uses that knowledge to frustrate those methods. No doubt, sophisticated criminals like Ace and Nicky exist in real life. But certainly, they are a small minority. After all, everyone knows that police collect fingerprints at crime scenes, yet people continue to fail to wear gloves when committing crimes. It's no secret that police can track a cell phone, yet people still carry them and leave them turned on when breaking the law.

This observation is important because it highlights the extent to which the anti-circumvention argument is mostly concerned with preserving law enforcement's effectiveness at the margins, in cases involving the behavior of the most sophisticated criminal actors.¹⁶⁷ When we decide that the anti-circumvention rationale should prevail, it is because we are concerned about the potential effect on investigations of a small minority of crimes; in the vast

166. *See, e.g.*, 18 U.S.C. § 2518(5) (2018) (“Every [wiretap] order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter”); UNITED STATES DEP’T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL PROCEDURES AND CASE LAW FORMS 12–14 (2005) (describing minimization requirements for wiretaps) <https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf> [<https://perma.cc/6JSU-XFCN>]; *id.* at 134 (“All monitoring will cease when it is determined that the monitored conversation is not criminal in nature.”). The government appears to have tried to address the circumvention risk by allowing periodic “spot checks” of minimized calls to determine whether they have turned to criminal matters. *See id.* at 134 (DOJ sample Title III roving wiretap application provides, “If an interception is minimized, monitoring agents all spot check insure that the conversation has not turned to criminal matters”).

167. Moreover, for reasons discussed presently, the most sophisticated criminal actors are the ones most likely to have developed countermeasures already.

majority of cases, there will be no difference.

This dynamic also explains why law enforcement, when making the anti-circumvention argument, so often raises the specter of the sophisticated terrorist.¹⁶⁸ The idea of a highly destructive and sophisticated criminal puts the argument on its strongest ground. But if we adopt the anti-circumvention argument because we are concerned about the high-tech terrorist, it means we will keep the public in the dark about how the police use technology even in the vastly more numerous cases where there is no criminal mastermind or grave public safety risk. The specter of terrorism drives secrecy with respect to run-of-the-mill policing.

The scene from *Casino* also illustrates a second key empirical point: the anti-circumvention argument only works if the information that would permit countermeasures is not already in the public domain—whether or not that information came from an official source. Suppose that the FBI's minimization rules for wiretaps were not in any law, court order, or other official document. Instead, imagine that the FBI's practice of not tapping routine calls was leaked to a reporter and published in the newspaper. It wouldn't matter to Ace and Nicky where the information came from, so long as they have the information they need to evade the FBI.

The lesson here is that the anti-circumvention rationale tends to crumble once information has come into the public domain, no matter how it gets there—whether by official disclosure, unauthorized leak, or outright theft. It also matters little whether information about a law enforcement technique is widely known or only available to those who want to find it. Because the anti-circumvention rationale presupposes sophisticated criminals, even relatively obscure knowledge—say, about the wiretapping practices of the FBI or the capabilities of the backscatter x-rays used in mobile vans—is enough to render further efforts to preserve secrecy futile.

Closely related is a third empirical limit on the anti-circumvention rationale: it may be the case that some piece of information is in the public domain that already alerts sophisticated criminals to take the same evasive measures that would be suggested if the police were to disclose secret information about their technique. Take the example of Stingrays. If malefactors already know that the government can surveil the location of cell phones by obtaining the cooperation of cell phone companies, then those would-be criminals already know how to take the appropriate countermeasure—i.e., turning the cell phone off or using a burner phone. But those are the same countermeasures that a criminal would adopt if they knew

168. See, e.g., *Grabell v. N.Y.C. Police Dep't*, 139 A.D.3d 477, 478–79 (N.Y. App. Div. 2016); *Morrison Affidavit*, *supra* note 13, at 1–3.

about Stingrays, which simply allow police to track cell phones without involving the cell phone company. In short, information in the public domain may already lead sophisticated criminals to take countermeasures that impede law enforcement's use of a secret technique. In such cases, secrecy serves no anti-circumvention purpose.

The anti-circumvention argument can also fail if disclosure simply does not permit the lawbreaker to learn anything that would assist him in evading law enforcement. Take the *Casino* example of FBI wiretapping again. Suppose that the FBI had rules that require it to dispose of recordings after a certain amount of time when recordings only contain benign, innocent conversations. It is hard to see how this rule could result in circumvention. Unlike the rules about switching off the wiretap that Ace and Nicky exploited, rules about record retention periods do not seem to create any risk of circumvention. The lesson here is that one cannot simply *assume* that disclosure of any and all information about law enforcement's capabilities and techniques will give rise to a threat of circumvention. The case needs to be made that disclosure will be useful to evade police.

Finally, the anti-circumvention argument can fail if the disclosure in question leaves uncertainty about how police will use the technique—and, therefore, how it could be circumvented. Ace and Nicky were able to exploit the FBI's minimization rules either because they knew precisely how much time the FBI agent could listen in before clicking off the call or because they could actually hear the FBI agent disconnecting the wiretap. The FBI could have mitigated the risk of circumvention by tweaking the technology or the rules in question. If the minimization rules prescribed no specific period of time before the wiretap was disconnected (or if the rules permitted random spot checks)¹⁶⁹ and if the wiretap device was completely silent, then there would have been no ready way for Ace and Nicky to evade the FBI. They would have used the phone at their peril, uncertain whether or not the FBI was in fact taping them. The example may generalize; in some cases, the nature of the technology or the rules in question can be difficult to circumvent because they are not sufficiently predictable or detectable.

So much for the empirical premises of the anti-circumvention argument; what about its normative underpinnings? On first blush, they seem unassailable: who in their right mind would want would-be lawbreakers to be able to evade law enforcement? If, as an empirical matter, disclosure would actually permit evasion of law enforcement, then surely it follows uncontroversially that we should oppose disclosure. There are at least two responses—one complicates the normative premise, and the other points out

169. As, indeed, DOJ guidelines currently allow. *See supra* note 166.

that competing normative commitments may swamp concerns to prevent circumvention.

First, there may well be circumstances where we actually do want to allow or even encourage evasion. The idea is that by allowing would-be lawbreakers to evade particular law enforcement techniques, we might channel them into less socially destructive behavior. Imagine, for example, that a city has outfitted its downtown area with technologically sophisticated surveillance cameras, automated license plate readers, perhaps also exotic chemical sensors, listening devices, and the like. Disclosing the capabilities of these devices might allow sophisticated lawbreakers to evade detection by these devices. The standard normative premise is that such evasion is a bad thing, so we should keep the capabilities of the devices secret. But the opposite normative premise may be more compelling: we may want people to know that law enforcement is watching in order to deter certain kinds of crimes or to displace crimes from a certain location.¹⁷⁰

Along similar lines, let's return to the story of Ace and Nicky. Because they knew the FBI's minimization procedures, they were able to evade the wiretap. But the wiretap nevertheless made it much harder for them to communicate, materially impeding their ability to conspire and giving the police other opportunities to surveil them. Ace and Nicky were forced to undertake elaborate measures in order to speak. Because they could not use the phone for any length of time without being wiretapped, they had to meet in person.¹⁷¹ In order to do so, they had to try to evade physical surveillance, switching cars multiple times in order to shake the FBI.¹⁷² They could only meet and speak undisturbed in exposed, dusty patches of desert outside town in order to avoid

170. There is mixed evidence about whether surveillance cameras have a deterrent effect on crime. Some studies have found a meaningful deterrent effect while others have not. The evidence is similarly mixed on the question of whether surveillance cameras serve merely to displace crime to unsurveilled locations. See, e.g., Eric L. Piza et al., *Analyzing the Influence of Micro-Level Factors on CCTV Camera Effect*, 30 J. QUANTITATIVE CRIMINOLOGY 237, 238–42 (2013) (reviewing the empirical literature on the deterrent effect of surveillance cameras and concluding that the evidence is mixed); Mikael Priks, *The Effects of Surveillance Cameras on Crime: Evidence from the Stockholm Subway*, 125 ECON. J. 289–91 (2015) (finding that surveillance cameras in subway stations deterred certain pre-planned crimes like pickpocketing, but tended to displace such crime to the immediate vicinity—e.g., outside subway entrances—beyond the view of the surveillance cameras); Joel M. Caplan et al., *Police-Monitored CCTV Cameras in Newark, NJ: A Quasi-Experimental Test of Crime Deterrence*, 7 J. EXPERIMENTAL CRIMINOLOGY 255, 264–71 (2011) (finding reductions in certain crimes in areas within the field-of-view of particular cameras, and finding no evidence that cameras served to displace the location of crimes).

171. See CASINO, *supra* note 162, at 1:52:40.

172. *Id.*

the possibility of physical or electronic surveillance.¹⁷³ In short, disclosing wiretap rules succeeded in putting the heat on Ace and Nicky, impairing their ability to make plans, even if it didn't succeed in intercepting every conversation.¹⁷⁴

This approach to policing is a kind of harm-reduction strategy. Police encourage or at least tolerate evasion of law enforcement in order to diminish opportunities for crime or to channel crime in less damaging directions. This approach may have much to say for it. Rather than requiring secrecy, it requires the opposite; the would-be criminal must know that law enforcement may be deploying a certain technique. As a result, it is not fair to assume that in every case evasion of law enforcement techniques will always be a bad thing, or that disclosure will always impair law enforcement objectives.¹⁷⁵

Second, even when we do actually want to prevent sophisticated criminals from evading law enforcement, we will often simultaneously hold competing normative commitments that move us to oppose secrecy. These competing values were explored in the prior Part: We want our law enforcement agencies to be amenable to democratic oversight and deliberation. We want courts, legislatures, and citizens to vet law enforcement techniques for compliance with the Constitution and other laws. We want to avoid circumstances where abuses proliferate in secret. We want law enforcement to be governed by laws and rules that are public. We want law enforcement to have the benefit of outside input and expert criticism. We want police to maintain trust and credibility with the people they serve. Secrecy impairs these goals. The decision to endorse anti-circumvention thus has major costs.

The upshot is that even if the anti-circumvention argument is sound and empirically justified, it is not conclusive. The decision whether to keep a law enforcement technique secret necessarily involves a value judgment—implicit

173. *Id.*

174. *Id.* (“Ace: The problem was, Nicky was not only bringin’ heat on himself, but on me too. The FBI watched every move he made. But he didn’t care. He just didn’t care.”).

175. In one interesting recent example, the New York Police Department threatened to bring legal action against Waze, a mapping app that crowdsources information from users, because the app allowed users to notify fellow drivers about the location of police drunk-driving checkpoints. NYPD argued that the app was allowing drivers to evade checkpoints and thereby impairing law enforcement. See Michael Gold, *Google and Waze Must Stop Sharing Drunken-Driving Checkpoints, New York Police Demand*, N.Y. TIMES (Feb. 6, 2019), <https://www.nytimes.com/2019/02/06/nyregion/waze-nypd-location.html> [<https://perma.cc/YB59-VYNH>]. Critics, however, pointed out that police checkpoints are more effective at deterring drunk driving if they are visible and public; the app might actually be *amplifying* the police’s intended deterrent effect by making checkpoints more public. See Hannah Bloch-Wehba, *The NYPD’s Misguided War on Waze*, SLATE (Feb. 13, 2019), <https://slate.com/technology/2019/02/nypd-waze-dwi-checkpoints-lawsuit-first-amendment.html> [<https://perma.cc/FL8X-93AC>].

or explicit—that anti-evasion concerns are weightier than the rest.

There is good reason to believe that most people do not assign normative priority to anti-circumvention concerns. Consider again Ace and Nicky: a world in which they did not know that the FBI's minimization rules required agents to stop listening to innocent telephone conversations would be a world in which the public was kept in the dark about the scope of the FBI's wiretap powers. In a very real sense, this would be a world of secret law; the rules governing the FBI's conduct would be hidden from the public. The public would not be able to know whether police could lawfully use a wiretap to intercept perfectly innocent conversations. Indeed, the public could not enact public rules to this effect because to do so would tip off mobsters. Of course, few people would be willing to endorse that kind of secrecy. We are simply not willing to accept that wiretapping should be governed by secret law in order to increase the effectiveness of the technique at the margins. To the contrary, we expect law enforcement to absorb any burdens on its investigatory capacity as a basic cost of democracy and rule of law.

Taking the contrary view—i.e., that anti-circumvention concerns generally outweigh competing values—leads to alarming conclusions. If our overriding concern were to prevent circumvention, then we would presumably think it justified to keep a good deal of Fourth Amendment law secret. After all, the Fourth Amendment imposes intricate limits on the police's ability to carry out various techniques. Sophisticated knowledge of Fourth Amendment rules may well allow a person to evade detection. For example, knowing that police cannot search inside a car's glovebox in the absence of consent or probable cause¹⁷⁶ may well allow an individual to avoid an arrest for drug possession. We do not typically lament this consequence. Instead, we accept it as a cost of the rule of law.

A thought experiment further illustrates the point. Imagine a world in which law enforcement has managed to keep *all* of its capabilities and techniques secret. The public does not know about how police can use fingerprints; it does not know about DNA testing; it does not know about wiretaps, etc. In that world, the would-be lawbreaker has no information that would allow him to evade law enforcement. If all we cared about was preventing such evasion, then we would presumably be comfortable with that state of affairs. But I think most of us recoil at the thought of living in a society

176. See *Carroll v. United States*, 267 U.S. 132, 153–54 (1925); *California v. Acevedo*, 500 U.S. 565, 580 (1991); Evan Levtow, *Locked Glove Compartments: Searchable or Stash Spots?*, 29 *TOURO L. REV.* 1115 (2013); John P. Besselman, *Locked Containers - An Overview*, FED. L. ENFORCEMENT TRAINING CTR., https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/4th-amendment/lockedcontainers.pdf [<https://perma.cc/GF25-RV7J>].

like that—one in which we are not allowed to know how the authorities can investigate any of us, lest some of us attempt to evade them.

Of course, in the real world, the public already knows a great deal about law enforcement's methods, and that knowledge cannot be erased from memory. But the question that arises—and the one that this Article grapples with—is how much we should be able to learn about *new* technologies, particularly technologies that can be deployed surreptitiously without revealing themselves to the target. If we would reject a world in which information about existing law enforcement techniques is secret, why do we accept a world in which information about new technologies can remain secret? A desire to prevent evasion of law enforcement does not alone answer the question. Answering in favor of secrecy implies a judgment that the anti-circumvention concern outweighs other considerations including, often, basic commitments to democratic accountability and rule-based governance.

V. ANTI-CIRCUMVENTION DOCTRINES

I now turn away from a theoretical exploration of the anti-circumvention argument in order to explore how the law actually protects the secrecy of law enforcement techniques. The principal sources of law in this area at the federal level are Exemption 7(E) of FOIA and the law enforcement evidentiary privilege.

A. THE FOIA EXEMPTION FOR LAW ENFORCEMENT “TECHNIQUES AND PROCEDURES”

FOIA imposes a presumptive requirement on the government to disclose any records in its possession upon request, including in theory records that might disclose law enforcement capabilities or techniques.¹⁷⁷ Of course, this disclosure mandate is not absolute; FOIA contains exemptions.¹⁷⁸ Key among these is the law enforcement exemption.¹⁷⁹ In particular, Exemption 7(E) permits federal agencies to withhold

records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk

177. *See* 5 U.S.C. § 552(a)(3)(A) (2018).

178. § 552(b).

179. § 552(b)(7).

circumvention of the law.¹⁸⁰

The scope of this exemption determines, to a great extent, how much official information the public can obtain about the capabilities of law enforcement technologies and how they are used. Exemption 7(E) is therefore worth examining in some detail.

Exemption 7(E) has been on the books in its current form since 1986,¹⁸¹ and it is frequently litigated. The case law interpreting the Exemption has given it a fairly broad scope. Courts have found that a wide range of information constitutes “techniques and procedures” or “guidelines” within the meaning of the exemption.¹⁸² Importantly, courts have permitted secrecy upon a modest showing that disclosure of a technique risks circumvention of law.

The D.C. Circuit, for example, has explicitly rejected the argument that the agency “has a high burden to specifically prove how the law will be circumvented.”¹⁸³ Instead, that court determined that “exemption 7(E) only requires that the [agency] demonstrate logically how the release of the requested information might create a risk of circumvention of the law.”¹⁸⁴ On this view, secrecy is justified if the agency is merely able to tell a coherent story about how circumvention “might” result. It is not a particularly high bar and, unsurprisingly, it permits a great deal of secrecy about novel technologies.¹⁸⁵

Some circuits have required even less. The Second and Ninth Circuits have taken the position that when it comes to information about “techniques and procedures,” no showing of risk of circumvention is required at all.¹⁸⁶ These

180. *Id.*; § 552(b)(7)(E).

181. The anti-circumvention rationale is also codified in the privilege for law enforcement investigative techniques, which has been recognized so far by a several circuit. *See* Smith, *supra* note 28, at 258–69 (detailing the development and present state of the law). In this Article, I focus solely on the FOIA exemption; future articles may include discussion of the privilege, as relevant.

182. *See, e.g.*, Blackwell v. FBI, 646 F.3d 37, 42 (D.C. Cir. 2011) (forensic computer examination methods); Hale v. Dep’t of Justice, 973 F.2d 894, 902–03 (10th Cir. 1992), *cert. granted, vacated & remanded on other grounds*, 509 U.S. 918 (1993) (information about polygraph examinations); Sheridan v. U.S. Office of Pers. Mgmt., 278 F. Supp. 3d 11, 21 (D.D.C. 2017) (source code and design manual for receiving and vetting security clearance forms); Showing Animals Respect & Kindness v. U.S. Dep’t of Interior, 730 F. Supp. 2d 180, 199–200 (D.D.C. 2010) (surveillance methods at wildlife refuge); Mayer Brown LLP v. Internal Revenue Serv., 562 F.3d 1190, 1192–93 (D.C. Cir. 2009) (settlement guidelines for tax audits).

183. *Mayer Brown*, 562 F.3d at 1194.

184. *Id.* (internal quotation and alterations omitted).

185. *See, e.g.*, Soghoian v. U.S. Dep’t of Justice, 885 F. Supp. 2d 62, 74–75 (D.D.C. 2012) (determining that information about Stingrays was exempt under Exemption 7(E)).

186. *See* Allard K. Lowenstein Int’l Human Rights Project v. Dep’t of Homeland Sec., 626 F.3d 678, 681–82 (2d Cir. 2010); Hamdan v. U.S. Dep’t of Justice, 797 F.3d 759, 778 (9th Cir. 2015).

courts have read the language in the exemption regarding the risk of circumvention to apply only to “*guidelines* for law enforcement investigations or prosecutions” and not to the earlier part of the exemption which covers “*techniques and procedures* for law enforcement investigations or prosecutions.”¹⁸⁷ The Second Circuit further clarified that “guidelines” in this context refers to “an indication or outline of future policy or conduct” and, specifically, “resource allocation” decisions about how to focus enforcement efforts.¹⁸⁸ “Techniques and procedures,” on the other hand, “refers to how law enforcement officials go about investigating a crime.”¹⁸⁹ Information about the existence and capabilities of law enforcement technologies may often fall in the latter category. Thus, on the Second Circuit’s view, police may be able to withhold information even if there is no plausible risk of circumvention at all.¹⁹⁰

The only consistent limit that the courts have recognized on the scope of Exemption 7(E) is that it “only exempts investigative techniques not generally known to the public.”¹⁹¹ In other words, information cannot be withheld if a technique is already public. The scope of this limitation, however, is contested

187. *Hamdan*, 797 F.3d at 777–78; *Sheridan*, 278 F. Supp. 3d at 22 (noting disagreement among courts about “whether the ‘risk of circumvention’ requirement applies to records containing ‘techniques and procedures’ or only to records containing ‘guidelines’”); *Pub. Emps. for Envtl. Responsibility v. U.S. Section, Int’l Boundary & Water Comm’n, U.S.-Mex.*, 740 F.3d 195, 204 n.4 (D.C. Cir. 2014) (same).

188. Allard K. Lowenstein Int’l Human Rights Project, 626 F.3d at 682.

189. *Id.*

190. *Id.* at 681–82. As the D.C. Circuit has noted, however, “given the low bar posed by the ‘risk circumvention of the law’ requirement, it is not clear that the difference matters much in practice.” *Pub. Emps. for Envtl. Responsibility*, 740 F.3d at 204 n.4. It is possible that the Second Circuit’s interpretation will be reconsidered in light of recent amendments to FOIA that now permit agencies to withhold information “only if the agency reasonably foresees that disclosure would harm an interest protected by an exemption.” FOIA Improvement Act of 2016, Pub. L. No. 114-185, § 2, 130 Stat. 538, 539 (2016) (codified at 5 U.S.C. § 552(a)(8)(A)(i) (2018)). Lower courts are interpreting this amendment to require agencies to identify some *harm* in order to successfully invoke exemptions. *See Rosenberg v. U.S. Dep’t of Def.*, 342 F. Supp. 3d 62, 77–79 (D.D.C. 2018) (holding that the new foreseeable harm standard imposes an additional burden on the government to justify withholding); *Judicial Watch v. U.S. Dep’t of Commerce*, 375 F. Supp. 3d 93, 100 (D.D.C. 2019) (same). The Second Circuit’s categorical approach to excluding “techniques and procedures” irrespective of any risk of circumvention or other articulated harm would probably not survive such an interpretation of the amendment. To date, however, no court has yet considered how amendment interacts with Exemption 7(E).

191. *See Rosenfeld v. U.S. Dep’t of Justice*, 57 F.3d 803, 815 (9th Cir. 1995); *accord Rugiero v. U.S. Dep’t of Justice*, 257 F.3d 534, 551 (6th Cir. 2001); *Davin v. U.S. Dep’t of Justice*, 60 F.3d 1043, 1064 (3d Cir. 1995); *Albuquerque Pub. Co. v. U.S. Dep’t of Justice*, 726 F. Supp. 851, 857–58 (D.D.C. 1989); *Malloy v. U.S. Dep’t of Justice*, 457 F. Supp. 543, 545 (D.D.C. 1978).

and applied inconsistently by the courts. It generally imposes only a weak constraint because the test only regards “generally known” information as sufficient to overcome secrecy. As a result, the most well-known and obvious techniques are more likely to fall outside Exemption 7(E),¹⁹² while courts are less likely to order disclosure with respect to novel law enforcement technologies at least until significant information about the technique has become public.¹⁹³ Indeed, courts have held that law enforcement can withhold even information about well-known techniques if the government contends that disclosure might risk circumvention.¹⁹⁴ In other words, the courts will rarely crack open a window on a police technique much wider than the window has already been opened by other forces.

Cases applying these standards demonstrate significant mismatches between Exemption 7(E) doctrine and the more rigorous explication of the logic of anti-circumvention offered in the prior Part.

For starters, the law does not typically require a strong explanation of the link between disclosure of the information at issue and the potential for circumvention. Where courts demand such an explanation, they only require a “logical” link between disclosure and circumvention.¹⁹⁵ To be sure, some courts have gone out of their way to take a close look at whether disclosure of particular details is likely to risk circumvention.¹⁹⁶ But in many instances, law

192. *See, e.g., Rosenfeld*, 57 F.3d at 815 (holding that the technique of using pretext phone calls was sufficiently well known that it could not be withheld under Exemption 7(E)); *Davin*, 60 F.3d at 1064 (“This exemption . . . may not be asserted to withhold routine techniques and procedures already well-known to the public, such as ballistic tests, fingerprinting, and other scientific tests commonly known.”) (internal quotation omitted); *Albuquerque Pub. Co.*, 726 F. Supp. at 857–58 (“[T]he government should avoid burdening the Court with an in-camera inspection of information pertaining to techniques that are commonly described or depicted in movies, popular novels, stories or magazines, or on television. These would include, it would seem to us, techniques such as eavesdropping, wiretapping, and surreptitious tape recording and photographing. Instead, the government should release such information to plaintiff voluntarily.”).

193. *See Soghoian*, 885 F. Supp. 2d at 74–75 (refusing to disclose any records regarding Stingrays in 2012). *But see* *ACLU of N. Cal. v. Dep’t of Justice*, 880 F.3d 473, 491–92 (9th Cir. 2018) (finding in 2018 that cell phone tracking technology was sufficiently well-known that certain records about Stingrays could not be withheld).

194. *See, e.g., Unidad Latina en Accion v. U.S. Dep’t of Homeland Sec.*, 253 F.R.D. 44, 53–54 (D. Conn. 2008) (weekly immigration arrest reports could be withheld under Exemption 7(E)); *Piper v. U.S. Dep’t of Justice*, 294 F. Supp. 2d 16, 30 (D.D.C. 2003) (finding documents that would disclose unspecified “logistical considerations” regarding polygraph tests could be withheld even though polygraphy is a well-known technique).

195. *N.Y. Times v. U.S. Dep’t of Justice*, 101 F. Supp. 3d 310, 319 (S.D.N.Y. 2015) (quoting *Blackwell v. FBI*, 646 F.3d 37, 40 (D.C. Cir. 2011)).

196. *See, e.g., Allard K. Lowenstein Int’l Human Rights Project v. U.S. Dep’t of Homeland Sec.*, 603 F. Supp. 2d 354, 354–55 (D. Conn. 2009), *aff’d*, 626 F.3d 678 (2d Cir. 2010); *ACLU*

enforcement can withhold information about “techniques and procedures” without showing any risk of circumvention at all.¹⁹⁷

The case law generally also takes a crude approach to assessing the effect of existing public-domain information that may render the risk of circumvention illusory. Rather than taking seriously the notion that secrecy may be futile because existing public-domain information already creates identical risks of circumvention, the case law takes the opposite tack: only if a technique is so well known and well publicized that it is common knowledge will secrecy be inappropriate.¹⁹⁸

Similarly, courts rarely take serious account of the likelihood that disclosure would allow criminals to develop genuinely new countermeasures. It is an unusual case where the court actually identifies potential countermeasures and considers whether such countermeasures would already be obvious based on existing publicly available information.¹⁹⁹

Courts also lack a nuanced approach to the probabilistic nature of alleged risks of circumvention. Whether disclosure will in fact encourage circumvention is rarely a certainty and usually a matter of conjecture. Rather than weighing the seriousness of the risk against countervailing concerns, courts adjudicating Exemption 7(E) claims simply end the inquiry once they have determined that there is some unspecified (and usually very small) probability of circumvention. There is no balance of the risks and rewards of disclosure.²⁰⁰

Perhaps most fundamentally, the existing case law fails to engage with the crosscutting value judgments implicated in secrecy determinations. There is no public interest “override.” The only value the exemption explicitly recognizes is law enforcement’s interest in confidentiality. The doctrine has no clear space for the weighty concerns about democratic accountability, separation of powers, or rule-based governance.²⁰¹ Those values, which otherwise animate FOIA, are often submerged in favor of the anti-circumvention rationale.²⁰² In

of N. Cal. v. Dep’t of Justice, 70 F. Supp. 3d 1018, 1036–39 (N.D. Cal. 2014), *aff’d*, 880 F.3d at 492.

197. See *supra* notes 186–190 and accompanying text.

198. See *supra* note 192 (collecting illustrative cases).

199. One outlier in this regard is Northern District of California’s decision rejecting the DOJ’s argument for withholding information about Stingrays, affirmed in relevant part by the Ninth Circuit. See *ACLU of N. Cal.*, 70 F. Supp. 3d at 1038.

200. See *supra* notes 182–183, 185, 192 (identifying illustrative cases).

201. See *supra* Sections III.A–D.

202. Indeed, in jurisdictions that do not require the government to show a risk of circumvention in order to keep techniques secret, there is not even a clear rationale for disregarding countervailing values: law enforcement gets to keep its techniques secret, whether

perhaps the starkest example of this problem, some courts have allowed the government to withhold records under Exemption 7(E) even if those records constitute the internal law that governs how an agency will operate.²⁰³ Thus, even the public interest in not having secret law has sometimes not been enough to defeat the anti-circumvention argument.²⁰⁴

The only true safety valve in the existing case law is the exception for information that is already in the public domain. But this is a crude and somewhat mystifying way of demarcating a line between proper and improper secrets. Whether or not some technique has entered popular culture and become widely familiar does not track whether sophisticated criminals will be able to exploit disclosures to evade detection. It also does not reflect the normative sacrifices involved in permitting secrecy. Just because something is not common knowledge does not mean it should remain secret. To return to a concrete example, the question of whether we should keep x-ray vans secret does not depend, as a normative matter, on the fact that NYPD has been very effective at hiding information about the vans. It depends instead on value judgments about democratic oversight and legal regulation of the public health and privacy issues that the technique implicates. Those concerns have little place in the current legal regime.²⁰⁵ Instead, by giving law enforcement the

or not disclosure would plausibly impair law enforcement's efforts. *See supra* notes 186–190 and accompanying text.

203. *See, e.g.,* ACLU v. U.S. Dep't of Justice, No. 12 CIV. 7412 WHP, 2014 WL 956303, at *1, *8 (S.D.N.Y. Mar. 11, 2014) (holding that government could withhold legal memorandum describing the parameters within which FBI could use unspecified location-tracking techniques even though the memorandum contained "the Government's interpretation of its constitutional obligations" with respect to such techniques); *N.Y. Times v. U.S. Dep't of Justice*, 101 F. Supp. 3d 310, 322 (S.D.N.Y. 2015) (holding that federal law enforcement agency could withhold emails describing "specific factual scenarios and . . . technical aspects of GPS tracking devices" even though it contained guidance governing use of such devices, which were already publicly known, because release would create unspecified "risk of a circumvention of the law"). *But see* ACLU of N. Cal., 880 F.3d at 492 (finding that Exemption 7(E) did not bar disclosure of documents that "describe the legal authorization necessary for obtaining location information, and describe legal arguments related to that acquisition").

204. *See* Manes, *supra* note 22, at 851–54.

205. Perhaps as a result of this doctrinal paradox, advocates seeking to shine a light on novel police technologies have mounted multi-pronged transparency campaigns in an effort to force disclosure of information. Such campaigns typically involve publicizing whatever information has managed to find its way into the public domain, publishing reports and articles about the technique in question, publicizing any discoveries and disclosures to the press to raise the profile of the issue, raising concerns in Congress, and generally sounding the alarm. Such publicity campaigns may ultimately shift perceptions to a sufficient degree that courts are willing to reject claims that disclosure will reveal a secret technique. *Compare* Soghoian v. U.S. Dep't of Justice, 885 F. Supp. 2d 62, 74–75 (D.D.C. 2012) (refusing disclosure about Stingrays) *with* ACLU of N. Cal., 880 F.3d at 492 (rejecting arguments against disclosure).

authority to keep techniques secret so long as they remain out of the public eye, the legal regime strongly incentivizes law enforcement to do everything it can to keep its technologies under wraps for as long as possible. In this way, it gives law enforcement significant power to decide when and how to disclose information about the capabilities it possesses and how they are used.

B. THE EVIDENTIARY PRIVILEGE FOR LAW ENFORCEMENT
INVESTIGATIVE TECHNIQUES

Historically, law enforcement did not enjoy any evidentiary privilege protecting information about its techniques.²⁰⁶ Since 1977, however, four federal circuit courts have squarely recognized a common law privilege that covers law enforcement techniques, and many district courts in other circuits have followed suit.²⁰⁷ In some of these jurisdictions, the privilege for law enforcement techniques is one component of a broader “law enforcement privilege” that, depending on the jurisdiction, serves to protect not just techniques but also investigatory files,²⁰⁸ “the identity of informer[s],”²⁰⁹ “witness and law enforcement personnel,” “the privacy of individuals involved in an investigation,” and “interference with an investigation.”²¹⁰ The courts have recognized these privileges in an exercise of their common law authority pursuant to Federal Rule of Evidence 501.

The appellate authorities do not elaborate in great detail on the scope of the privilege for law enforcement techniques but suggest that its sweep is similar to that of FOIA Exemption 7(E). Indeed, a number of the decisions explicitly analogize the evidentiary privilege to Exemption 7(E), even while recognizing that the considerations at stake in the FOIA, which is concerned with policing the line between secrecy and disclosure to the general public, are different and less acute than those at stake with the privilege, which can prevent defendants in criminal cases from obtaining evidence for use in their

206. See Smith, *supra* note 28, at 233–34.

207. See United States v. Piroosko, 787 F.3d 358, 365–67 (6th Cir. 2015) (applying qualified “law enforcement privilege” to law enforcement technique); *In re Dep’t of Investigation of N.Y.*, 856 F.2d 481, 483–84 (2d Cir. 1988) (recognizing “law enforcement privilege” the purpose of which is “to prevent disclosure of law enforcement techniques and procedures”); United States v. Cintolo, 818 F.2d 980, 1001–03 (1st Cir. 1987) (holding that qualified privilege protects “nature and location of electronic surveillance equipment”); United States v. Van Horn, 789 F.2d 1492, 1507–08 (11th Cir. 1986) (same); Black v. Sheraton Corp. of Am., 564 F.2d 550, 541–47 (D.C. Cir. 1977) (recognizing “law enforcement evidentiary privilege” against “disclosure of documents that would tend to reveal law enforcement investigative techniques or sources”).

208. See, e.g., Dellwood Farms v. Cargill, Inc., 128 F.3d 1122, 1125–28 (7th Cir. 1997).

209. See, e.g., Roviario v. United States, 353 U.S. 53, 60, 66–67 (1957).

210. See, e.g., *In re Dep’t of Investigation of N.Y.*, 856 F.2d at 484.

defense.²¹¹

The Eleventh Circuit has explained the basis for the privilege in perhaps the most explicit terms. In *United States v. Van Horn*, a criminal defendant sought disclosure of information about what type of microphone was used to surveil him and where the microphone had been hidden in a particular room.²¹² The case was decided in 1986, at a time when hidden microphones or “bugs” were already well known. Nevertheless, the court held that “the privilege applies equally to the nature and location of electronic surveillance equipment,”²¹³ on the reasoning that

[d]isclosing the precise locations where surveillance devices are hidden or their precise specifications will educate criminals regarding how to protect themselves against police surveillance. Electronic surveillance is an important tool of law enforcement, and its effectiveness should not be unnecessarily compromised. Disclosure of such information will also educate persons on how to employ such techniques themselves, in violation of Title III.²¹⁴

The court’s reasoning rested entirely on these generalized concerns. It did not provide (or, it appears, demand) any particularized explanation about how disclosure of details about the hidden microphone in question could compromise the effectiveness thereof in a future investigation. It also did not consider whether disclosure would have created any meaningful additional risk of evasion in light of information already in the public domain.²¹⁵

Subsequent decisions in the lower courts apply the privilege broadly to prohibit disclosure of information about all manner of technology, even techniques that are decades old and well known to anyone who has ever watched a police procedural. Thus, courts have withheld information about pen registers,²¹⁶ hidden sound and video recording devices,²¹⁷ and polygraph

211. *See, e.g., Black*, 564 F.2d at 545–46.

212. *Van Horn*, 789 F.2d at 1507.

213. *Id.* at 1508.

214. *Id.*

215. *See id.*

216. *United States v. Garey*, No. 5:03-CR-83, 2004 WL 2663023, at *1 (M.D. Ga. Nov. 15, 2004) (privilege covered information about “the nature and details pertaining to the use of the pen register and trap and trace devices”).

217. *United States v. Alimehmeti*, 284 F. Supp. 3d 477, 493 (S.D.N.Y. 2018) (privilege covered “methodology used to facilitate recordings” between undercover officer and suspect); *United States v. Djokich*, No. CR 08-10346-MLW, 2016 WL 927145, at *5 (D. Mass. Mar. 7, 2016) (privilege covered specific “types of computers, recording devices, and software used by the government” to record telephone conversations); *United States v. Farha*, No. 8:11-CR-115-T-30MAP, 2012 WL 12964913, at *2–3 (M.D. Fla. Sept. 27, 2012) (privilege likely applies to “the device or devices . . . used in making . . . recordings [of defendant]; the operating

examinations.²¹⁸ The privilege has also been successfully invoked to prevent disclosure of information about newer technology including Stingrays²¹⁹ and various forms of surveillance software.²²⁰

In these cases, courts often require little if any demonstration that disclosure of the information sought would create a significant risk of circumvention. In many cases, it is enough simply that the material in question pertains to a law enforcement technique.²²¹ Similarly, courts rarely inquire whether the technique in question is already well known to the public, or whether information in the public domain already creates the risk of circumvention that the government seeks to avoid.²²² In fact, in one recent case concerning Stingrays, a court found that the privilege prohibited disclosure even while it acknowledged elsewhere in its opinion that the criminal defendant had amassed a treasure trove of detail from public sources regarding the operation of the device.²²³ In this respect, the privilege often

manual for these devices including their spec sheets; the batteries” and related equipment); *United States v. Little*, No. 09-20673-CR, 2010 WL 11570441, at *2–3 (S.D. Fla. Jan. 21, 2010) (privilege covered “inspection of the recording device” used to record defendant); *United States v. O’Neill*, 52 F. Supp. 2d 954, 963 (E.D. Wis. 1999), *aff’d sub nom. United States v. Warneke*, 199 F.3d 906 (7th Cir. 1999) (“recording and monitoring equipment used to transmit and record [defendant]”).

218. *Shah v. Dep’t of Justice*, No. 15-15232, 2017 WL 4812585, at *1 (9th Cir. Oct. 25, 2017) (privilege covered “charts, graphs, and raw data associated with [polygraph] examination” of criminal defendant).

219. *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 1002 (D. Ariz. 2012) (information about cell-site simulator was held to be privileged).

220. *United States v. Matish*, 193 F. Supp. 3d 585, 592 (E.D. Va. 2016) (privilege encompasses source code for “network investigative technique” that allowed government to identify a person’s computer and location); *United States v. Pirosko*, 787 F.3d 358, 365 (6th Cir. 2015) (privilege applied to law enforcement software used to investigate illegal file-sharing); *United States v. Hoeffener*, No. 4:16CR00374 JAR/PLC, 2017 WL 3676141, at *18 (E.D. Mo. Aug. 25, 2017) (privilege covered source code, manuals, and other information regarding software used to conduct investigations on the BitTorrent file-sharing network).

221. *See, e.g., Shah*, 2017 WL 4812585, at *1; *Little*, 2010 WL 11570441, at *2–3; *Garey*, 2004 WL 2663023, at *4. *But see United States v. Taylor*, No. 3:14-00015, 2015 WL 9274934, at *3 (M.D. Tenn. Dec. 18, 2015) (expressing skepticism that information about a GPS tracking device fell within scope of privilege because of the familiarity of the technology and technique involved); *Ibrahim v. Dep’t of Homeland Sec.*, No. C 06-00545 WHA, 2013 WL 1703367, at *5 (N.D. Cal. Apr. 19, 2013) (“screening procedures and requirements for being placed on the No-Fly and other watch lists” could be disclosed, despite claim of privilege, pursuant to an “attorney’s eyes only” protective order limiting further dissemination).

222. *See, e.g., Matish*, 193 F. Supp. 3d at 601; *Shah*, 2017 WL 4812585, at *1; *Djokich*, 2016 WL 927145, at *5; *Farha*, 2012 WL 12964913, at *2–3; *Little*, 2010 WL 11570441, at *2; *Garey*, 2004 WL 2663023, at *4.

223. *Rigmaiden*, 844 F. Supp. 2d at 999 (noting that defendants’ “filings contain extensive technical data regarding cell tower simulation technology [including] product brochures,

mirrors the broadest version of Exemption 7(E), which requires no showing of circumvention risk at all.²²⁴

Unlike in the FOIA context, however, the evidentiary privilege for law enforcement techniques is not an absolute bar to disclosure but is instead subject to a balancing test that weighs “[t]he public interest in nondisclosure . . . against the need of a particular litigant for access to the privileged information.”²²⁵ If a criminal defendant or civil plaintiff can make a strong showing of need, the privilege may be overcome. Courts have established various tests in the civil²²⁶ and criminal²²⁷ contexts to determine whether disclosure is required despite a claim of privilege. In general, however, the privilege will be overcome only upon a showing that evidence is necessary or important to a party’s case and that there are no alternative means for the party to make the relevant point or argument.²²⁸

In principle, the possibility of overcoming a claim of privilege could allay some of the concerns about secrecy that were canvassed above. But, in practice, this safety valve is often stuck closed. Courts have placed a heavy burden on criminal defendants to identify in advance particular arguments they wish to make and to demonstrate that, without disclosure, they would not be able to make them.²²⁹ It is difficult, however, to know in advance which secret facts might support a compelling constitutional or statutory argument. A technology may operate in ways that are opaque to the defendant and yet deeply constitutionally suspect. Moreover, even where it appears that a party will be able to make the requisite showing of need and lack of alternative means, the government can avoid disclosure (and subsequent litigation) by making narrow strategic concessions that obviate the need for disclosure.²³⁰

patent applications, articles, websites, and textbooks [that] show the manner in which cell tower emulation occurs”).

224. See *supra* note 186 and accompanying text.

225. *In re City of New York*, 607 F.3d 923, 945 (2d Cir. 2010) (quoting *In re Sealed Case*, 856 F.2d 268, 272 (D.C. Cir. 1988)).

226. See, e.g., *id.* at 945 (party seeking disclosure “must show (1) that its suit is non-frivolous and brought in good faith, (2) that the information sought is [not] available through other discovery or from other sources, and (3) that the information sought is important to the party’s case”) (internal quotation and alteration omitted).

227. See, e.g., *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987) (criminal defendant must make “a sufficient showing of need,” which “requires a case by case balancing process controlled by the fundamental requirements of fairness”) (internal quotations and citations omitted).

228. See generally *United States v. Alimehmeti*, 284 F. Supp. 3d 477, 493–94 (S.D.N.Y. 2018) (synthesizing common elements of tests for overcoming privilege).

229. See, e.g., *United States v. Little*, No. 09-20673-CR, 2010 WL 11570441, at *2 (S.D. Fla. Jan. 21, 2010); *Alimehmeti* 284 F. Supp. at 494.

230. See *infra* notes 232–236 and accompanying text (discussing *Rigmaiden*, 844 F. Supp. 2d at 982).

Perhaps as a result, there are few reported decisions in which a party succeeded in overcoming the government's claim of privilege.²³¹

These concerns were highlighted most vividly in the high-profile case of Daniel Rigmaiden, a criminal defendant charged with making numerous fraudulent tax filings. Rigmaiden managed to piece together evidence strongly suggesting that the government had discovered his location using a Stingray device.²³² Rigmaiden sought discovery of information about the Stingray technology and how it was used. He intended to use that information in support of a suppression motion, which would have tested whether using a Stingray requires a warrant and whether the police's use in his case had exceeded the scope of the judicial authorization they had actually obtained.²³³ The case promised to be the first time the federal government would face a Fourth Amendment challenge to its use of a Stingray device.

Ultimately, however, the court held that even Rigmaiden could not demonstrate sufficient "need" to displace the law enforcement privilege, in large part because the government made a number of strategic concessions in order to avoid disclosure.²³⁴ Among other things, the government conceded, solely for purposes of that case, that its investigative actions had constituted a "search" for purposes of the Fourth Amendment; it also conceded certain specific details about how Rigmaiden alleged the device had been used.²³⁵ Having made those concessions, Rigmaiden's "need" for information about the capabilities and deployment of the government's Stingray technology evaporated. By making these strategic concessions, the government avoided any actual disclosures about its capabilities and evaded any judicial

231. *See, e.g.*, *State v. Harris*, 819 So. 2d 844, 846 (Fla. Dist. Ct. App. 2002) (location from which police surveilled suspect was not privilege because the officer's testimony on the matter was essential to the defense and there was no videotape of the surveillance); *United States v. Foster*, 986 F.2d 541, 543–44 (D.C. Cir. 1993) (same); *United States v. Taylor*, No. 3:14-00015, 2015 WL 9274934, at *4 (M.D. Tenn. Dec. 18, 2015) (expressing skepticism that information about a GPS tracking device fell within scope of privilege because of the familiarity of the technology and technique involved); *Ibrahim v. Dep't of Homeland Sec.*, No. C 06-00545 WHA, 2013 WL 1703367, at *5 (N.D. Cal. Apr. 19, 2013) ("screening procedures and requirements for being placed on the No-Fly and other watch lists" could be disclosed, despite claim of privilege, pursuant to an "attorney's eyes only" protective order limiting further dissemination); *United States v. Wright*, No. 2:08-CR-5-02, 2008 WL 8797841, at *4 (D. Vt. Nov. 3, 2008) (claim of privilege was overcome with respect to "training and certification records that reflect the [drug detection] dog's accuracy and reliability").

232. Cale G. Weissman, *How An Obsessive Recluse Blew the Lid off the Secret Technology Authorities Use to Spy on People's Cellphones*, BUS. INSIDER (June 19, 2015), <http://www.businessinsider.com/how-daniel-rigmaiden-discovered-stingray-spying-technology-2015-6> [<https://perma.cc/8S9R-X95U>].

233. *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 989 (D. Ariz. 2012).

234. *Id.* at 995–96, 1005.

235. *Id.*

determination on the core Fourth Amendment questions.²³⁶

Thus, despite vigorous litigation with an extraordinarily dogged and well-prepared criminal defendant, the courts and the public remained in the dark about both the legal boundaries and technical powers of the government's Stingray technology. In the mine run of criminal cases, secret technologies will go undetected or unchallenged because defense lawyers, carrying heavy caseloads, usually have little capacity to piece together the highly technical methods potentially used against their clients and few resources to employ experts, who are generally necessary to build a legal challenge.²³⁷

In short, the law enforcement privilege stands as a major obstacle to disclosure of novel law enforcement technologies and to adjudication of the legal rules that govern them. The scope of the privilege exceeds what a concern to prevent circumvention could justify. Even in the context of criminal cases, which fully engage the due process rights of individual defendants, courts have been reluctant to allow disclosure. The law thus erects barriers against external oversight even where police use novel technologies to obtain criminal convictions.

VI. REFORMING THE LAW OF SECRET LAW ENFORCEMENT TECHNOLOGIES

Any meaningful reform agenda must address two basic problems caused by anti-circumvention secrecy: (1) secrecy reallocates power away from legislatures and courts to the police, leaving the police free to use intrusive technologies without meaningful checks; and (2) it distorts the relationship between citizens and the government by expanding the investigatory and informational powers of government at the expense of an unwitting citizenry. This Article offers two strategies to achieve such reform. The first targets the legal doctrines that provide the government overbroad powers to resist disclosure in the face of requests from the public. The second requires affirmative disclosure and public comment so that legislatures, courts, and the public can engage in the process of regulating novel technologies before they

236. *See id.* at 999–1002. In a subsequent decision, the Court found that the warrant the government had obtained was valid, despite the fact that the warrant application gave no indication to the magistrate judge that the search was to be conducted using a Stingray device. *See United States v. Rigmaiden*, No. 08-cr-814, 2013 WL 1932800, *33–34 (D. Ariz. May 8, 2013).

237. Recognizing this problem, some non-profit organizations and legal services offices have begun to devote specialized staff to build challenges to novel surveillance technologies. *See, e.g.*, NAT'L ASS'N OF CRIM. DEF. LAW, *Nation's Criminal Defense Bar Launches Initiative to Educate, Litigate Privacy Challenges in a Digital Age* (2018), <https://www.nacdl.org/Fourth-Amendment-Center-Launch/> [<https://perma.cc/W5W9-738L>].

come into routine use.

A. NARROWING THE SCOPE OF ANTI-CIRCUMVENTION SECRECY

As we have seen, existing doctrines protect far more information about novel technologies than a rigorous application of the anti-circumvention argument justifies. Courts endorse secrecy based on too little evidence about how disclosure would actually lead to circumvention.²³⁸ The straightforward response to this problem would be to require courts to demand more from law enforcement. Why not amend the laws to impose a higher burden of justification on law enforcement agencies? Why not simply urge judges to exercise their existing powers more vigorously?

This straightforward solution is intuitively appealing, but it is likely doomed to fail. The history of FOIA is a history of judicial deference to agencies.²³⁹ Despite Congress' textual mandate that courts must review secrecy claims "de novo" and that the "burden is on the agency to sustain its action,"²⁴⁰ courts have been reluctant to vigorously guard the line between the public's business and proper secrets. As a general rule, courts defer to government claims and do not demand detailed or highly persuasive justifications.²⁴¹ Prior efforts to strengthen the judicial role by amending FOIA have failed. In 1974, Congress went so far as to override a veto by President Ford in order to empower judges to vigorously oversee government secrecy claims.²⁴² The effort failed; scholars and commentators agree that judges quickly reverted to a very deferential posture.²⁴³ In light of this experience, textual amendments purporting to require courts to scrutinize the government's justifications more closely are not likely to make a difference, except perhaps at the margins.²⁴⁴

238. See Part V.

239. See, e.g., Margaret B. Kwoka, *Deferring to Secrecy*, 54 B.C. L. REV. 185, 211–35 (2013); Margaret B. Kwoka, *Deference, Chenery, and FOIA*, 73 MD. L. REV. 1060, 1067–74 (2014).

240. 5 U.S.C. § 552(a)(4)(B) (2018).

241. See, e.g., *Larson v. Dep't of State*, 565 F.3d 857, 865, 867–88 (D.C. Cir. 2009); *ACLU v. U.S. Dep't of Def.*, 901 F.3d 125, 133–34, 136 (2d Cir. 2018).

242. See David E. Pozen, *Freedom of Information Beyond the Freedom of Information Act*, 165 U. PA. L. REV. 1097, 1118–19 (2017).

243. See, e.g., *id.*; Kwoka, *Deferring to Secrecy*, *supra* note 239, at 199–200; Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131, 156–63 (2006); Nathan Slegers, Comment, *De Novo Review Under the Freedom of Information Act: The Case Against Judicial Deference to Agency Decisions to Withhold Information*, 43 SAN DIEGO L. REV. 209, 213–18 (2006); Paul R. Verkuil, *An Outcomes Analysis of Scope of Review Standards*, 44 WM. & MARY L. REV. 679, 687–93 (2002).

244. A recent amendment to FOIA which requires the government to show "reasonably foresee[able] . . . harm," in order to invoke exemptions may reign in the broadest applications of Exemption 7(E). 5 U.S.C. § 552(a)(8)(A)(i)(I) (2018); see *supra* note 190. But that amendment is unlikely to prompt courts to be more skeptical in general of government claims that disclosure will risk circumvention.

If increasing the justificatory burden on the government (or the stringency of judicial oversight) is unlikely to succeed, what will? Some authors have proposed that courts should be empowered to weigh the public interest in disclosure against the government's exemption claims.²⁴⁵ This would empower judges to consider all of the arguments in favor of transparency canvassed in the previous Parts. No doubt, some courts would use this doctrinal tool to order disclosure. However, it seems more likely that courts will not wield this authority particularly aggressively, just as they have failed to vigorously exercise their (already very strong) textual authority to conduct *de novo* review.

The reason for this has to do with the prevailing judicial culture and self-conception about the proper role of judges—particularly federal judges. Many judges today resist the idea that it is *their* responsibility—rather than the agency's—to make value judgments about whether disclosure is warranted or predictive judgments about the likely harm of disclosure. This is especially true in matters of law enforcement and security, where deference is especially pronounced.²⁴⁶ A public interest override cuts against the grain of this prevailing judicial culture. It asks the judge to make *her own* value judgment and prediction about the relative harms and benefits of disclosure. In a similar way, Congress's requirement of *de novo* review in FOIA cases imagined that the judge would make *her own* judgment about whether secrecy was warranted. But in practice, that provision has resulted in judges serving only as a mild check on the “plausibility” or “logic” of the agency's decision.²⁴⁷ All such doctrinal constructs depend on the idea that the judge will take the ultimate secrecy determination out of the agency's hands—that the court will make its own determination, not merely sit in review of the agency's. But that role is not one that many contemporary judges seem willing to play. It simply does not appear to comport with the dominant views about the (circumscribed) role and (limited) competence of judges, especially in matters of law enforcement and security.

A different sort of reform, however, may be more effective. What we need are additional *categorical* limits on what falls within the FOIA exemption for law enforcement techniques and the corresponding privilege. Categorical rules do

245. See Katie Townsend & Adam A Marshall, *Striking the Right Balance: Weighing the Public Interest in Access to Agency Records Under the Freedom of Information Act*, in TROUBLING TRANSPARENCY: THE HISTORY AND FUTURE OF FREEDOM OF INFORMATION 226, 233–41 (David E Pozen & Michael Schudson, eds. 2018).

246. See, e.g., *ACLU*, 901 F.3d at 134, 136; *ACLU v. Dep't of Def.*, 628 F.3d 612, 624 (D.C. Cir. 2011); *ACLU v. Dep't of Justice*, 681 F.3d 61, 76 (2d Cir. 2012). *But see* *N.Y. Times Co. v. U.S. Dep't of Justice*, 765 F.3d 100, 116–17 (2d Cir. 2014) (finding that the government had waived various national security exemptions to disclosure because it had already released a version of the document it sought to withhold).

247. See *supra* notes 239–243 and accompanying text.

not ask the courts to weigh the relative strength of the government's case for secrecy against the public's interest in disclosure. Instead they require the courts simply to determine what the withheld material *is* and whether it falls inside or outside a particular description. This type of analysis casts judges in the more comfortable role of sorting facts into legal categories—exempt vs. non-exempt—rather than making predictive judgments or value judgments about the relative harms and benefits of disclosure. It is therefore more likely to be an effective way to rein in existing anti-circumvention doctrines.

This Article offers four potential categorical limits on the scope of secrecy. First, FOIA exemptions and the law enforcement privilege should not allow police to keep secret the very existence of a secret technology. It is one thing for police to keep the public in the dark about how the police use some technology, it is quite another for police to conceal from the public that the technology exists at all. In the latter case, the public (and criminal defendants) cannot even know that there is something to be worried about and so secrecy serves to utterly frustrate any external checks. These kinds of secrets—known as “deep secrets”—are widely regarded as problematic, perhaps even raising constitutional problems because they circumvent the basic democratic levers of our constitutional system.²⁴⁸

Second, anti-circumvention doctrines should not allow the government to keep secret the *rules* that govern how a technology may be used. In other words, the anti-circumvention argument cannot justify “secret law.” This limit on secrecy reflects the idea that secret law is fundamentally at odds with the rule of law and basic notions of due process, particularly where rules in question regulate government powers that affect the public.²⁴⁹

A prohibition on secret rules also has at least some pedigree in existing case law. In one of its early FOIA decisions, the Supreme Court held that the government's power to withhold privileged “deliberative process” materials under FOIA could not justify withholding “‘opinions and interpretations’ which embody the agency's effective law and policy.”²⁵⁰ This decision rested

248. See David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 288–92, 305–06 (2010); see also Manes, *supra* note 22, at 817–26.

249. See generally Manes, *supra* note 22 (examining the problems with secret law in depth); LON FULLER, *THE MORALITY OF LAW* (rev. ed. 1969) (arguing that one of the principles essential to the “internal morality of law” is that laws cannot be kept from the public); Jonathan Hafetz, *A Problem of Standards?: Another Perspective on Secret Law*, 57 WM. & MARY L. REV. 1 (2016); Dakota S. Rudesill, *Coming to Terms with Secret Law*, 7 HARV. NAT'L SEC. J. 241 (2015); Sudha Setty, *No More Secret Laws: How Transparency of Executive Branch Legal Policy Doesn't Let the Terrorists Win*, 57 KAN. L. REV. 597 (2009); ELIZABETH GOITEIN, BRENNAN CENTER FOR JUSTICE, *THE NEW ERA OF SECRET LAW* (2016).

250. *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 153 (1975) (internal quotation omitted).

explicitly on the idea that FOIA itself “represents a strong congressional aversion to ‘secret [agency] law’ . . . and represents an affirmative congressional purpose to require disclosure of documents which have ‘the force and effect of law.’ ”²⁵¹ Lower courts subsequently extended this “secret law” doctrine to another FOIA exemption that—at the time, at least—permitted secrecy of documents that would “risk circumvention of agency regulations” in general.²⁵²

Unfortunately, however, the courts have thus far declined to extend this anti-secret law principle to the rules that govern investigative techniques, in particular. In one early case, the D.C. Circuit determined that a Bureau of Alcohol, Tobacco, and Firearms manual “designed to establish rules and practices for agency personnel, i.e., law enforcement investigatory techniques” and which “ha[d] some effect on the public-at-large” nevertheless did not constitute “secret law” because the “manual is used for predominantly internal purposes.”²⁵³ Recent cases continue this trend.²⁵⁴ But these cases have come under intense criticism,²⁵⁵ and their reasoning does not seriously grapple with the idea that the government can act according to secret rules—and therefore short-circuit democratic checks—simply in order to preserve an advantage in the small slice of criminal investigations where it might make a difference.

Third, the government should not be permitted to withhold facts about the capabilities of a technology—or the manner in which it is used—insofar as those facts are necessary to determine whether the Fourth Amendment has been violated. The basic idea is that the government should not be able to evade accountability for potential violations of the fundamental law of the country by keeping those violations secret. In order to operationalize this limit, the party seeking disclosure could be required to come forward with a colorable argument that the technology is being used in such a way that it

251. *Id.* (quoting K. Davis, *The Information Act: A Preliminary Analysis*, 34 U. CHI. L. REV. 761, 797 (1967), and H.R. REP. NO. 1497, at 7 (2019)) (alteration in original).

252. *See Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 670 F.2d 1051, 1067–75 (D.C. Cir. 1981) (construing FOIA Exemption 2, 5 U.S.C. § 552(b)(2)); *Jordan v. U.S. Dep’t of Justice*, 591 F.2d 753, 781–82 (D.C. Cir. 1978) (Bazelon, J., concurring) (same). The Supreme Court has since ruled that these cases rested on a mistaken interpretation of Exemption 2 under which there was a general exemption for disclosures of any records that could lead to circumvention of agency regulations. *See Milner v. Dep’t of the Navy*, 562 U.S. 562, 573–76 (2011). The Court clarified that FOIA only includes one specific anti-circumvention exemption—the one for law enforcement techniques found in Exemption 7(E). *Id.* at 575.

253. *Crooker*, 670 F.2d at 1073.

254. *See, e.g., ACLU v. Dep’t of Justice*, No. 12 Civ. 7412(WHP), 2014 WL 956303, at *8 (S.D.N.Y. Mar. 11, 2014) (rejecting “secret law” carve-out to Exemption 7(E)).

255. *See, e.g., Jameel Jaffer & Brett Max Kaufman, A Resurgence of Secret Law*, 126 YALE L.J. F. 242, 248 (2016) (discussing cases that have allowed agencies to keep their effective law and policies secret).

violates the Fourth Amendment; the government would then be required to disclose facts necessary to illuminate the claim. In the FOIA context, this change would probably require legislation; nothing in the current text suggests that constitutional considerations are relevant. With respect to the evidentiary privilege, courts could simply relax the showing of “need” that is required for a criminal defendant to overcome a claim of privilege. Instead of imposing a high bar, courts could simply rule that disclosure is required whenever there is a colorable claim the Fourth Amendment may have been violated.²⁵⁶

Finally, secrecy about the capabilities of novel technologies could expire once a technology comes into routine use—as opposed to merely experimental use. The idea here is that it makes sense for law enforcement to have some leeway to try out novel technologies and deliberate about their effectiveness without necessarily opening itself up to scrutiny. However, once the police put a technology into routine use, the public’s interest in understanding the capabilities of law enforcement outweigh the police’s interest in preventing circumvention.²⁵⁷ To be sure, this could make law enforcement’s task harder at the margin. To the extent that disclosure tips off sophisticated criminals to adopt countermeasures they were not otherwise taking, law enforcement’s task will be more difficult. But, ultimately, that may be a price we must pay to live in a democratically accountable society, and it is a price that we already happily pay with respect to all of the humdrum investigative tools that police have been using for decades—from wiretaps to polygraphs to fingerprints. It is unclear why we should be willing to extend to *new* technologies a shroud of secrecy that we seem quite able to live without with respect to old, well-known technologies.

B. PUBLIC NOTICE AND COMMENT FOR NOVEL INVESTIGATIVE TECHNOLOGIES

The more ambitious solution to the problem of secret investigative techniques redistributes regulatory power from the police to legislatures and courts through mandatory, affirmative disclosure requirements. Under the status quo, the police can obtain and deploy new technologies without necessarily putting anyone else on notice. This is especially true with respect

256. Courts would also have to rebuff government efforts to evade disclosure by making strategic concessions, as the government did in the *Rigmaiden* case. *See supra* notes 232–236 and accompanying text.

257. As I use the term here, “routine” use does not mean frequent use, but instead that the technology is among the tools that the police have at their disposal should they choose to use it. Democratic accountability and public deliberation concerns do not dissipate just because a technology is used relatively infrequently. In fact, some of the most intrusive technologies may be used infrequently because they are costly, complex, or controversial. This may be the case with respect to x-ray vans; we don’t know.

to surveillance tools because they are less visible to the public than other police technologies. If the police adopt tasers, for example, the public will be able to see them. However, if the police begins using facial recognition software to analyze footage from existing surveillance cameras, that can easily remain invisible to the public for years. Doctrinal solutions that merely tighten up FOIA exemptions and privileges, like those proposed above, will only produce greater transparency if potential litigants learn enough about a particular technology to be able to bring affirmative challenges in court seeking disclosure.

I propose instead to flip the status quo by requiring law enforcement to issue a public notice whenever it acquires a new technology, before the technology goes into regular use. The notice would, at a minimum, document the capabilities of the technology, describe its purpose, and disclose the proposed policies governing its use, including the circumstances in which it can be used (and the internal or external authorizations required) and the restrictions on retention, access, or use of information collected using the technology. The notice could also require the police to identify and assess potential effects on individual rights to privacy, non-discrimination, and other civil liberties, and to include an analysis of the proposed technology's compliance with applicable constitutional and statutory restrictions. The basic idea is that the notice would provide the information necessary to permit the legislature and the public to exercise meaningful control and oversight over the deployment of novel technologies.

In conjunction with the public notice, the public would have the opportunity to comment on the proposed policy and for the legislature to hold hearings or otherwise engage in oversight. The policy would not go into effect until and unless the police considered and addressed the comments and issued a final policy. In form and function, the process would be akin to the notice and comment process that is familiar from many areas of administrative law practice.²⁵⁸

This proposal has the virtue of requiring a democratic conversation about the proper place of a technology *at the outset*, before it has become entrenched. It eliminates secrecy at the outset by imposing an affirmative disclosure requirement on law enforcement. It also recalibrates how the anti-circumvention argument may be deployed to resist transparency. By enacting a general notice-and-comment regime governing novel surveillance technologies, the legislature effectively makes a judgment that legislative oversight and democratic accountability values should generally prevail over

258. See Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 137–49 (2016).

anti-circumvention concerns.

Moreover, the notice-and-comment process permits some flexibility as to the level of granularity at which the police disclose the policies governing a surveillance technology. The idea is that the police could disclose policies that are granular and detailed enough to permit the public to understand (and, potentially, criticize) how the novel technology will be used, but not so granular that a criminal could readily use the policy as a detailed roadmap to evade the new technology. I have argued elsewhere, in an article examining the phenomenon of secret law, that adjusting the level of granularity at which the government discloses its rules and legal interpretations can be a powerful way to modulate the tension between democratic interests in transparency and governmental interests in secrecy.²⁵⁹ In the context of a notice-and-comment process, there is the possibility of modulating the degree of secrecy in just this way: if the police pitch public notice in terms that are not sufficiently specific or concrete, the legislature and public will be in a strong position to demand greater transparency before the technology comes into use.

The affirmative notice and comment process also shifts the terrain on which we adjudicate arguments about anti-circumvention secrecy. In the ordinary FOIA process, *courts* have to make a legal judgment, *ex-post*, about whether disclosure of a particular piece of information falls within the exempt category of “techniques and procedures.” As we have seen, courts have been reluctant to consider countervailing policy considerations favoring transparency when making those judgments. Indeed, courts have been very deferential to law enforcement secrecy arguments.²⁶⁰

By contrast, the affirmative notice-and-comment process creates a new locus for decisions about secrecy outside of the courts and away from legal wrangling over the scope of the relevant FOIA exemptions or other doctrines. Instead, the notice-and-comment process requires *legislatures* (and, by extension, the public) to make a *policy* judgment about whether additional disclosure is necessary in order to permit meaningful and sufficient public accountability. The idea is that the give-and-take between the legislature, the public, and law enforcement is likely to shift the boundary between secrecy and transparency to a place that may provide more meaningful disclosure than courts have been willing to offer. The hope is that in this way the public’s interest in transparency and accountability will have more weight in decisions

259. See Manes, *supra* note 22, at 837–38.

260. See, e.g., Pozen, *supra* note 242, at 1099; Kwoka, *Deferring to Secrecy*, *supra* note 239, at 211–35; Mark Rumold, *The Freedom of Information Act and the Fight Against Secret (Surveillance) Law*, 55 SANTA CLARA L. REV. 161, 179 (2015); Robert P. Deyling, *Judicial Deference and De Novo Review in Litigation over National Security Information under the Freedom of Information Act*, 37 VILL. L. REV. 67, 93 (1992).

about where to draw the curtain around police capabilities or policies.

This reform proposal draws on the recent “administrative turn” in scholarship regarding police regulation and oversight. In particular, this proposal builds on the recent work of Professor Christopher Slobogin, who has proposed administrative law processes like notice-and-public-comment as a means to regulate “panvasive,” suspicionless police practices like drug-testing programs or traffic checkpoints that affect large segments of the population.²⁶¹ This Article proposes, in effect, that this administrative law approach should govern all novel surveillance technology.

These types of reforms are having some success on the ground. Indeed, in offering this reform agenda this Article is not writing on a blank slate. Not only does Slobogin’s recent work prefigure the idea of notice and comment, but the proposal here closely mirrors legislative proposals developed by a broad coalition of civil rights organizations that is pursuing reforms in state and local legislatures around the country.²⁶² Indeed, over the past two years, surveillance transparency laws that include some or all of essential elements described above have been enacted in several cities and counties,²⁶³ and at least two states have taken up legislation that would have statewide effect.²⁶⁴ While there do not yet appear to be efforts at the federal level to require this kind of surveillance transparency, it is possible at least to imagine Congress enacting public notice-and-comment requirements as a condition of federal funding to

261. Slobogin, *supra* note 258, at 93; *cf.* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 60 STAN. L. REV. 1039, 1047–49 (2016).

262. *See, e.g.*, ACLU, COMMUNITY CONTROL OVER POLICE SURVEILLANCE: TECHNOLOGY 101, *supra* note 8; *The Public Oversight of Surveillance Technology (POST) Act: A Resource Page*, BRENNAN CENTER FOR JUSTICE (June 12, 2017), <https://www.brennancenter.org/analysis/public-oversight-police-technology-post-act-resource-page> [<https://perma.cc/AK8T-VHYH>]; Michael Price & Alyssa Derosa, *New York City is Making its Citizens Safer by Overseeing Police Technology*, HUFFINGTON POST, Apr. 3, 2017, https://www.huffingtonpost.com/entry/new-york-city-is-making-its-citizens-safer-by-overseeing-police-technology_us_58e23f04e4b0ba359596583b [<https://perma.cc/Y6SH-8SLC>]. The ACLU has developed model legislation that it hopes to enact in local and state legislatures around the country. *See* ACLU, *An Act to Promote Transparency and Protect Civil Rights and Civil Liberties with Respect to Surveillance Technology* (2017), <https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf> [<https://perma.cc/E3UL-GQHH>].

263. *See, e.g.*, Acquisition and Use of Surveillance Technologies, SEATTLE MUN. CODE §§ 14.18.010–.070 (Aug. 2, 2017); Surveillance Technology Use and Community Safety Ordinance, BERKELEY MUN. CODE §§ 2.99.010–.110 (Mar. 13, 2018). *See generally* ACLU, *An Act to Promote Transparency and Protect Civil Rights and Civil Liberties with Respect to Surveillance Technology*, *supra* note 262.

264. *See* S.B. 21, 2017–2018 Leg. Sess. (Ca. 2016); S.B. 1186 (Ca. 2018); An Act to Promote Transparency with Respect to Surveillance Technology, Me. S. Paper 268, Legis. Doc. 823 (introduced Mar. 2, 2017).

states and local law enforcement agencies.²⁶⁵ It is also of course possible for the federal government to enact a surveillance transparency law to govern its own law enforcement agencies. In any event, there is a building movement for reform. Through this Article, I throw my hat in the ring with the advocates pursuing surveillance transparency laws.

VII. CONCLUSION

Secret innovation in law enforcement surveillance technology poses a challenge to democratic accountability as well as legislative and judicial oversight of police. Law enforcement has justified this secrecy by arguing that it is necessary to prevent criminals from circumventing novel police techniques. The practice on the ground and the decisions of courts, however, have produced a degree of secrecy that outstrips this justification. They have also failed to properly consider powerful countervailing values favoring transparency. The result is that the public, legislatures, and courts are largely shut out of the conversation even while we are seeing explosive growth in police surveillance technologies that raise profound constitutional, statutory, and policy problems.

Put simply, a concern to prevent criminals from misusing information has led to its suppression, even though that information is essential to democratic governance. In order to maintain meaningful external checks and public accountability, it will be necessary to tame the anti-circumvention argument, narrow its scope, and flip presumptions of secrecy so that transparency prevails in the face of speculation that disclosure might somehow, somewhere create an opportunity for evasion.

265. The federal government has distributed billions of dollars to federal and state law enforcement to fund police equipment. *See generally* NATHAN JAMES, CONG. RES. SERV., EDWARD BYRNE MEMORIAL JUSTICE ASSISTANCE GRANT PROGRAM (2013); Alicia Parlapiano, *The Flow of Money and Equipment to Local Police*, N.Y. TIMES (Dec. 1, 2014), https://www.nytimes.com/interactive/2014/08/23/us/flow-of-money-and-equipment-to-local-police.html?_r=0 [<https://perma.cc/QE8S-LGFA>].

UNCONSCIONABILITY 2.0 AND THE IP BOILERPLATE: A REVISED DOCTRINE OF UNCONSCIONABILITY FOR THE INFORMATION AGE

Amit Elazari Bar On[†]

ABSTRACT

In the information age, where fewer goods and more innovations are produced, intellectual property law has become the most crucial governing system. Yet, rather than evolving to fit its purpose, it has seemingly devolved—standard form contracts, governing countless creations, have formed an alternative de facto intellectual property regime. The law governing the information society is often prescribed not by legislators or courts, but rather by private entities, using technology and contracts to regulate much of the creative discourse. The same phenomena persist in other emerging areas of information law, such as data protection and cybersecurity laws.

This Article offers a new analytical perspective on private ordering in intellectual property (IP) focusing on the rise of IP boilerplate, the standard form contracts that regulate innovations and creations. It distinguishes between contracts drafted by the initial owners of the IP (such as End-User-License-Agreements (EULAs)) and contracts drafted by nonowners (such as platforms' terms of use), and highlights the ascendancy of the latter in the user-generated content era. In this era, the drafter of the contract owns nothing, yet seeks to regulate the layman adherent's creations, and sometimes even to redefine the contours of the public domain.

Private ordering is expanding its governing role in IP, creating new problems and undermining the rights that legislators bestow on creators and users. While scholars often discuss the problems caused by IP boilerplate, solutions are left wanting. Inter-doctrinal solutions have been unjustly overlooked. IP scholars reject general contract doctrines as ill-

DOI: <https://doi.org/10.15779/Z38PG1HP01>

© 2019 Amit Elazari Bar On.

[†] Lecturer, UC Berkeley School of Information. This Article is based on my J.S.D (Doctor of Science of Law) Dissertation (UC Berkeley School of Law) filed December 2018 and portions of the paper Amit Elazari Bar On, *Copyright and the Greater System of Rights: Utilizing Contractual Concepts to Solve Intellectual Property Problems in Standard-Form Contracts*, 29 INTEL. PROP. L.J. 83 (2016). I am grateful for their comments on earlier versions to Lior Zemer, Peter Menell, Steven Davidoff Solomon, Deirdre Mulligan, Chris Jay Hoofnagle, Robert P. Merges, Molly Shaffer Van Houweling, Mark Lemley, David Nimmer, Aaron Perzanowski, Orly Lobel, Mark Gergen, Aviv Gaon, Guy Rub, Eric Goldman, Ted Mermin, Miriam Bitton, Amir Huri, Abraham Drassinower, Niva Elkin-Koren, Uri Hacoen, and the participants of the 2017 Annual Intellectual Property Scholars Conference, the 2017 Internet Law Work-in-Progress Workshop, the 2017 Bay Area Scholars Work-in-Progress Workshop, the J.S.D. Workshop held on Berkeley Law on Oct. 4, 2017. All errors remain my own.

equipped. Contracts scholars discard IP considerations, perpetuating consumerist perspectives. This dichotomy, deepened by the preemption doctrine, has led to the underutilization of the prominent doctrine governing standard form contracts: unconscionability. Yet, in the aftermath of *ProCD*, preemption has failed to solve problems created by contracts in IP settings, while unconscionability has evolved from a legal marginality to a coherent concept.

Inspired by the Israeli purposive approach to unconscionability, this analysis aims to resurrect unconscionability as a pragmatic solution to problems created by IP boilerplate. According to this solution, the question of unconscionability is examined by asking, substantially, whether the provision benefits the relevant IP policies or negates them. Drawing on moral foundations, this solution seeks to avoid utilitarian biases and invites discourse between competing approaches. As a legal standard applicable to various relationships, even those that are non-consumer-based, it accommodates the dynamic adjustments often required when IP policies seek to address contemporary problems.

While IP scholarship has discarded unconscionability as ill-equipped, this Article suggests that it is an accessible solution that can accommodate extra-contractual notions. Precisely because the doctrine is rooted in contract law, its flexibility and broad applicability are why it could serve as a universal solution to myriad problems created by appropriating contracts. Adopting Unconscionability 2.0 would allow U.S. case law to align the roots of the doctrine with the needs of the information age.

TABLE OF CONTENTS

I.	INTRODUCTION	571
II.	INTRODUCING IP BOILERPLATE: WHEN THE FINE PRINT UNDERMINES CREATIVITY AND INNOVATION	586
A.	THE ADHERENT-USER AND THE ADHERENT-CREATOR DISTINCTION	591
B.	ADHERENT-USER IP BOILERPLATE	595
1.	<i>Some Examples from Fair Use Waivers to the “Right-to-Repair” Your Smartphone</i>	<i>596</i>
2.	<i>The Rise (and Fall?) of the “Patent-Wrap” Boilerplate: Limitations on the First-Sale Doctrine, Ownership, and the Sale/License Sham</i>	<i>606</i>
C.	ADHERENT-CREATOR IP BOILERPLATE	610
1.	<i>Social Networks and User-Generated Content: Cognitively Overburdened Creators</i>	<i>610</i>
D.	THE TECHNOLOGICAL BOILERPLATE: UNCONSCIONABILITY BY DESIGN.....	612
E.	A GAME OF CATCH? SOME EXISTING SOLUTIONS AND THE IP BOILERPLATE PARADOX.....	614
III.	UNCONSCIONABILITY 1.0—A BRIEF HISTORY OF AN ALIENATING DISCOURSE BETWEEN CONTRACTS AND IP LAW.....	622
A.	WHY UNCONSCIONABILITY?	622
B.	THE UNDERUTILIZATION OF THE UNCONSCIONABILITY DOCTRINE IN IP SETTINGS.....	629
1.	<i>The Chicken and the Egg: The Dismissal of Unconscionability in IP Scholarship.....</i>	<i>629</i>
2.	<i>The Preemption Doctrine and the Contract-IP “Dichotomy”</i>	<i>636</i>
3.	<i>A Limited Tool Set: From ProCD and Preemption to Lexmark and Exhaustion</i>	<i>646</i>
4.	<i>The Dialogue of the Deaf.....</i>	<i>653</i>
IV.	UNCONSCIONABILITY 2.0—TOWARDS A REVISED DOCTRINE OF UNCONSCIONABILITY DERIVED FROM INTELLECTUAL PROPERTY RATIONALES.....	657
A.	THE PROPOSED DOCTRINE OF UNCONSCIONABILITY 2.0	658
1.	<i>Theoretical Background and Comparative Insights: Adopting a Purposive Approach to Unconscionability</i>	<i>658</i>
2.	<i>Unconscionability 2.0: The Advantages of the Purposive Approach.....</i>	<i>666</i>
3.	<i>The Adoption of Unconscionability 2.0 in U.S. Law</i>	<i>676</i>
4.	<i>Unconscionability 2.0 in Negotiated Contracts and Between Sophisticated Parties.....</i>	<i>678</i>
B.	A ROBUST VISION FOR UNCONSCIONABILITY 2.0.....	681
1.	<i>Presumptions of Unconscionability 2.0.....</i>	<i>681</i>

2.	<i>Creating an Affirmative Right of Action</i>	684
3.	<i>Some Case Studies—The Application of Unconscionability 2.0</i>	687
4.	<i>Unconscionability 2.0 in Other Technological Realms</i>	694
5.	<i>Unconscionability 2.0: A “Wild Card” or a Winning Hand—Some Objections and Responses</i>	697
V.	CONCLUSION	702

“[The] deployment of boilerplate to achieve widespread cancellation of user rights contributes to democratic degradation . . . the [E]ULA can override . . . what the federal intellectual property regimes enacted as appropriate user rights.”¹

— Margaret Jane Radin

“[T]he rule-making process regarding the use of information is privatized, and the legal power to define the boundaries of public access to information is delegated to private parties.”²

— Niva Elkin-Koren

“[T]he fine print is not a contract It is nothing but paperwork and should have the legal fortune of junk mail.”³

— Omri Ben-Shahar

“[F]reedom of contract must mean different things for different types of contracts. Its meaning must change with the social importance of the type of contract”⁴

— Friedrich Kessler

1. MARGARET JANE RADIN, *BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW* 168–69 (2012).

2. Niva Elkin-Koren, *A Public-Regarding Approach to Contracting Copyrights*, in *EXPANDING THE BOUNDARIES OF INTELLECTUAL PROPERTY: INNOVATION POLICY FOR THE KNOWLEDGE SOCIETY* 191, 192 (Rochelle Dreyfuss et al. eds., 2001) [hereinafter Elkin-Koren, *Contracting Copyrights*].

3. Omri Ben-Shahar, *Regulation Through Boilerplate: An Apologia*, 112 MICH. L. REV. 883, 883 (2014) (reviewing RADIN, *supra* note 1) [hereinafter Ben-Shahar, *Regulation Through Boilerplate*].

4. Friedrich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629, 642 (1943).

I. INTRODUCTION

In early 2013, at the age of twenty-seven, an emerging creator from Jerusalem directed a video-clip of the famous Dylan song, “Like a Rolling Stone.”⁵ The video allowed viewers a unique interactive experience as they flipped between sixteen channels of a simulated TV and watched how characters of their choice lip-synced the lyrics of the song. The passive spectators became active creators, and millions began generating their own creative versions of the song via the innovative interactive platform. Time magazine declared, “[f]inally, a video worthy of the song,”⁶ and the young creator was selected as one of the fifty most creative people of 2014.⁷

Three years earlier, Vania Heymann, the creator of the video, began his visual communication studies at Bezalel, a renowned Israeli design academy. As part of his coursework, Heymann created videos and uploaded them to YouTube.⁸ His videos quickly became viral, as did his name. Little did Heymann know that according to Bezalel’s IP policy, he was infringing on the academy’s rights. The prior written consent of the academy president, accompanied by the recommendation of a designated committee, is required for such publication.⁹ That is, at least according to the general take-it-or-leave-

5. Vania Heymann, *Bob Dylan “Like a Rolling Stone”*, EKO (Nov. 19, 2013), <https://interlude.fm/v/M3b5GV> [<https://perma.cc/TL8B-KANJ>].

6. Melissa Locker, *Watch: An Incredible New Video for Bob Dylan’s “Like A Rolling Stone”*, TIME (Nov. 19, 2013), <http://entertainment.time.com/2013/11/19/watch-an-incredible-new-video-for-bob-dylans-like-a-rolling-stone/> [<https://perma.cc/JCB4-QMPC>].

7. Alexandra Jardine, *Creativity 50 2014: Vania Heymann*, ADVERTISINGAGE (Dec. 29, 2014), <http://adage.com/article/creativity-50/creativity-50-2014-vania-heyman/296277/> [<https://perma.cc/4WJV-XQKK>]. The video sparked a celebrated international career, and in 2016 Heymann co-directed MTV’s award-winning video “Up & Up” for the famous band, Coldplay.

8. Some of the videos were uploaded with a short subtitle, noting they were made as “homework assignment[s].” See, e.g., Vania Heymann, *my watering can*, YOUTUBE (Oct. 22, 2010), <https://www.youtube.com/watch?v=SzzW1wm3qPg> [<https://perma.cc/2LT7-44XY>] (“My first homework assignment for Bezalel school of arts & design, Jerusalem.”).

9. According to Bezalel’s IP Policy, all of the IP rights of the student are assigned (with no reward) to the institution if the creation or the invention is conceived “as part of” or “during” her studies. In addition, the student is explicitly warned not to present, publish, copy, or make commercial use of the creation (although, theoretically, she is no longer the owner of the creation, and does not own such rights), for a period of seven years following her graduation without the explicit consent of the academy president, accompanied by the recommendation of a designated committee. See Bezalel Academy of Arts and Design, *Students’ Regulations Including Discipline Rules and Copyright Annex B*, www.bezalel.ac.il/res/2012andupmisc/shnaton/2015/takanon.pdf [<https://perma.cc/J5BX-GDEN>] § 1, 4 [hereinafter *Bezalel’s Policy*].

it contract Heymann signed as a sine qua non for his admission.¹⁰

Were YouTube required to, it could have immediately and “in its sole discretion,” removed the allegedly infringing content, regardless of whether it was just or fair.¹¹ This, according to the broad prerogative YouTube retains under its Terms of Use (ToU): yet another standard form contract¹² creators often do not read.¹³

Luckily, this did not happen. Nor did Bezael try to enforce the broad language under their policy, which assigns (with no reward) all rights in Heymann’s homework assignments to the academic institution.¹⁴ This young creator, much like many others, probably did not pay careful attention to the boilerplate language purporting to govern his intellectual creations. He did not know that the fate of his innovative work of art—at least according to the contractual language—is not for him to decide. But, imagine a different scenario in which Heymann never uploaded his work, in fear of the boilerplate language prohibiting him from doing so. Would millions of viewers have been denied the joy of interacting with Dylan’s song three years later? Would this innovative creation have lived to reach its audience?

10. The boilerplate specifically alerts the student that her agreement to the policy is “a pre-condition to her admission,” and a signature is required “for the sake of good order.” *Id.* at pmbl.

11. Until May 25, 2018, section 7.B of YouTube’s ToU stated:
 YouTube reserves the right to decide whether Content violates these Terms of Service for reasons other than copyright infringement, such as, but not limited to, pornography, obscenity, or excessive length. YouTube may at any time, without prior notice and in its sole discretion, remove such Content and/or terminate a user’s account for submitting such material in violation of these Terms of Service.

Terms of Service, YOUTUBE (June 9, 2010), <https://web.archive.org/web/20130105115726/https://www.youtube.com/static?template=terms> [<https://perma.cc/XQ86-5JTN>].

12. Standard form contracts (or boilerplate) are contracts that are offered to consumers with no room for negotiation, on a “take-it-or-leave-it” basis. The drafter enjoys supremacy in both negotiation power and information, and the consumer usually does not spend much time reading the agreement prior to agreeing to it. *See generally* RADIN, *supra* note 1.

13. In general, users of social networks, similar to other non-drafters, are boundedly rational decisionmakers. They almost never read the platforms’ ToUs. Interestingly, one qualitative researcher suggests that even emerging artists who rely on social platforms to maintain exposure and attract new audiences are unaware of the terms and often have not “spent time considering” them. *See* Liz Dowthwaite et al., *How relevant is copyright to online artists? A qualitative study of understandings, coping strategies, and possible solutions*, 21 *FIRSTMONDAY* 5 (2016), <http://firstmonday.org/ojs/index.php/fm/article/view/6107/5457> [<https://perma.cc/VA33-QRD7>].

14. By, for example, issuing a takedown notice to YouTube under the DMCA. 17 U.S.C. § 512 (2018).

In the information society, our thoughts have become a commodity; our ideas have become products, and intangibles have become our most valuable resources. As a boundless discourse of ideation and response fuels creation on a multitude of platforms, an economy of innovation thrives—but who dictates the rules of the game? Although IP laws should guide society’s response to this evolution, reality proves that too often, these rules are ultimately not prescribed by courts and legislators, but rather by private entities.

The countless creations uploaded by users to social platforms such as YouTube, Instagram, and Vimeo and the innovations created by students worldwide are just a partial list of intellectual resources governed by private ordering. The law of the platform,¹⁵ meaning the terms of use drafted by a few lawyers, is the “private law”¹⁶ that governs most contemporary cultural discourse. Contracts, which no one reads, are probably the most prominent vessel used for the purpose of assigning and governing IP rights in the information age; they govern countless innovations and essentially have formed an alternative de facto IP regime. I call them IP boilerplate: a form of “modern”¹⁷ standard form contract combined with a “core case of democratic derogation,”¹⁸ focusing on regulating innovations and creations in direct

15. This term was coined by Orly Lobel, who used it in order to define more broadly the new, unconventional regulatory theory that governs the platform economy. *See* Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 87 (2016) (focusing on a specific aspect of this emerging field of law—the manner in which platforms use boilerplate language in order to bypass traditional IP regimes). I further claim that existing legal regimes cannot continue to ignore the two fundamental, interdependent features of the “law of the platform”: the ever-expanding use of standard form contracts as a regulation mechanism, and the fact that such contracts regulate more user-creators, innovations, and creations than ever before. In Lobel’s terms, standard form contracts serve an integral part of the “regulation-innovation nexus,” and therefore should be used in order to promote innovations, not monopolize or stifle creativity, which is inconsistent with the purpose of IP laws. *See id.* at 92.

16. *See* Kessler, *supra* note 4, at 640.

17. Four and a half decades ago, Slawson claimed, “[i]f contract law is to provide the basis for a democratic system of private law and for a competitive economy which works in the interests of consumers . . . it must take into account the . . . conditions under which modern contracting takes place.” W. David Slawson, *Standard Form Contracts and Democratic Control of Lawmaking Power*, 84 HARV. L. REV. 529, 565–66 (1971). Since then, modern contracting has, in fact, changed. Society is challenged by an evolving version of modern contracting—a new form of contract that seeks to assume control over expressions and content resources.

18. Indeed, as Radin noted, IP boilerplate bestows upon private parties the power to rewrite IP laws. RADIN, *supra* note 1, at 169. Radin refers to EULAs, but her argument applies to IP boilerplate in general. She also suggests that “the large number of people affected seem to matter in this case,” aggravating the problem of democratic degradation. *Id.* The complexity and variety of rights regulated under contract, as well as the fact that IP rights confer monopolistic control and their entitlement affects society in general, matters as well.

interaction with IP policies.

The scope of innovation and the variety of legal matters governed by standard form contracts in IP settings is inconceivable. It ranges from multi-billion-dollar software codes¹⁹ to patients' recommendations on Yelp; from the ability of researchers to tinker, perform reverse engineering, and test for vulnerabilities in products such as voting machines,²⁰ to farmers' "right to repair" and circumvent the software embedded in their own tractors; from Instagram and Reddit's ability to commercialize social-media content²¹ to the ability of Lexmark consumers to resell or dispose of patented print cartridges. These contracts determine whether Donald Trump Jr. had a legal right to tweet the famous Skittles picture created by the photographer and refugee, Kittos, accompanied by an anti-refugee political statement.²²

19. Much of the scholarship devoted to the contract/copyright interplay was focused on this type of IP boilerplate, the End-User-License Agreement (EULA) that accompanies software products. This is an adherent-user type of contract in which the drafter, the owner of the copyright, seeks to limit the ability of the user to access, use the product, reverse engineer the software, or even resell the product.

20. See, e.g., MULLIGAN ET AL., BERKELEY CTR. FOR LAW & TECH., UC BERKELEY SCHOOL OF INFO. & THE INT'L COMPUT. SCI. INST., CYBERSECURITY RESEARCH: ADDRESSING THE LEGAL BARRIERS AND DISINCENTIVES 6 (2015), <https://www.ischool.berkeley.edu/sites/default/files/cybersec-research-nsf-workshop.pdf> [<https://perma.cc/4JZX-JJ8Q>] (explaining that while "the urgency of the cybersecurity threat has grown to affect more types of products and services . . . contractual prohibitions on reverse engineering have proliferated"). The report describes how private ordering affects essential research efforts by limiting tinkering and testing. For example, contractual terms sought to limit most of the testing required for research that exposed critical vulnerabilities in voting machines. *Id.* at 1, 23. While the Librarian of Congress recently exempted "good-faith security" research from the DMCA prohibitions on copyrighted systems circumvention, contractual language often continues to ban researches from doing so, subjecting them to breach of contract claims. See 17 U.S.C. §§ 1201(1)(A), (C) (2018); 37 C.F.R. § 201 (2018). The exemption is "solely for the purpose of good-faith security research" that "does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986." *Id.* Therefore, contractual limitations may frustrate the purpose of this exemption if they create a basis for liability under other laws.

21. Under Reddit's previous ToS, users submitting content to the platform granted an irrevocable perpetual license to the platform (and "others" of its choice) to display and reproduce their creations "in any medium and for any purpose, including commercial purposes." *Reddit User Agreement* § 18, REDDIT (May 27, 2016), <https://web.archive.org/web/20180404004414/https://www.reddit.com/help/useragreement> [<https://perma.cc/G5M2-499W>] (effective until March 2018, when Reddit changed its ToS).

22. Kittos created a photographic image of colored candies inside a white bowl and posted it on his Flickr account. Trump Jr. tweeted the image with the accompanying text: "If I had a bowl of skittles and I told you just three would kill you. Would you take a handful? That's our Syrian refugee problem." See Chiara Palazzo, *Donald Trump Jr compares Syrian refugees to a bowl of Skittles*, TELEGRAPH (Sep. 20, 2016), <http://www.telegraph.co.uk/news/2016/09/20/donald-trump-jr-compares-syrian-refugees-to-a-bowl-of-skittles/>

Sometimes these contracts involve patents, such as the “patent-wrap” label agreement used to impose post-sale restrictions on secondary markets.²³ Other times they involve copyrighted creations, as in the case of social media platforms’ ToU and software EULAs. They are the mechanism through which patentees expand their monopolistic control beyond traditional patent law boundaries.²⁴ They range from blunt monopolization of traditional elements of the public domain, such as facts and data, to what has become perhaps the broadest waiver of moral rights in the history of humanity.²⁵ Now, as digital society becomes more focused on data abuses amid news of data breaches and privacy violations that consume media headlines,²⁶ the effects of boilerplate

[<https://perma.cc/2P8R-FDNC>]. Kittos filed a takedown notice under the DMCA, the tweet has been removed, and a copyright infringement suit is being litigated in Illinois Northern District Court. *See* Complaint, *Kittos v. Donald J. Trump For President, Inc.*, No. 16-cv-9818, (N.D. Ill. Oct. 18, 2016). Kittos alleges that the photo was published and used without his permission. The answer to this question partially depends on whether the platform to which Kittos originally uploaded the content allows the creators, under its ToS, to choose the license they seek to grant in uploaded content.

23. The “patent-wrap” is my paraphrase of the famous “shrinkwrap” agreement (the paper agreements that accompany software CD packages, and unilaterally define the terms of the software IP license); the “clickwrap” agreement (the online version of such contracts that require the user to manifest “assent” by clicking “I accept”); the “browsewrap” agreements (similar licenses that are presented on websites and are “hyper-linked” to the service/product downloaded); and the latest addition—“tap-wraps,” which is the smartphone version of the clickwrap agreement. *See* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CALIF. L. REV. 1239 (1995). The “patent-wrap” is a “wrap contract” under Nancy Kim’s definition, since it is “a unilaterally imposed set of terms which the drafter purports to be legally binding and which is presented to the nondrafting party in a nontraditional format.” *See* NANCY KIM, *WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS 2* (2013); *see also* Leon E. Trakman, *The Boundaries of Contract Law in Cyberspace*, 38 PUB. CONT. L.J. 187 (2008) (describing wrap contracts and exploring, from a contractual standpoint, how unconscionability was analyzed in their context).

24. *See, e.g.*, *Lexmark Int’l, Inc. v. Impression Prods.*, 816 F.3d 721 (Fed. Cir. 2016), *rev’d*, 137 S. Ct. 1523 (2017).

25. Under platforms such as Vimeo and Spotify, users waive their moral rights under terms of use. *See Vimeo Terms of Service Agreement* § 9.2, VIMEO (Oct. 6, 2017), <https://vimeo.com/terms> [<https://perma.cc/8T52-S8FZ>]; *see also* *Spotify Terms and Conditions of Use* § 7, SPOTIFY (Sep. 9, 2015), <https://www.spotify.com/us/legal/end-user-agreement/> [<https://perma.cc/V5CA-ZQ3J>].

26. *See, e.g.*, Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 744 (2018) (explaining how the issue of data breaches “cries out for attention,” how the number of breaches is on the rise, and proposing a conceptual framework for data-breach harms); *see also* *6 Months, 945 Data Breaches, 4.5 Billion Records*, CONSUMER BUS. REV. (Oct. 9, 2018), <https://www.cbronline.com/news/global-data-breaches-2018> [<https://perma.cc/J7FN-RS8C>] (explaining that “[t]he equivalent to 291 records were stolen or exposed every single second in the first half of 2018, Gemalto’s Breach Level Index shows,” a total of 4.5 Billion Records for the first half of 2018); Troy Hunt, “—have i been pwned?,” <https://haveibeenpwned.com/> [<https://perma.cc/EWV3-V6RH>] (allowing

controlling the use of information—operating in the shadow of the law—are garnering more scholarly and regulatory attention.²⁷

Although widespread in both virtual and non-virtual realms, these contracts usually remain hidden on a deserted web page that creators and users never read.²⁸ In some cases, they take the form of a clickwrap agreement that users spend less than one second reading before they click on so they can use the “free” service of the platform.²⁹ In other cases, they are one of many other

every user, including the reader of this Article, to check if their account has been compromised in a data breach database encompassing 6,729,238,699 pwned [owned, in information security jargon] accounts, to date).

27. A prominent example is EU General Data Protection Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and the recently adopted California Consumer Privacy Act. *See* General Data Protection Regulation, 2016 O.J. (L 119) (EU) (repealing Directive 95/46/EC (General Data Protection Regulation)); California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2018) (CCPA). The EU General Data Protection Regulation and the California Privacy Act of 2018 include robust regulations as to how and what companies should disclose with respect to their information collection practices, but more importantly police certain prohibited practices regardless of disclosure and users’ consent. They embrace, to some extent, the notion of bounded rationality. *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 156 (2017); *see also* Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is And What It Means* (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3254511 [<https://perma.cc/FX5S-JXPY>] (providing a comprehensive overview of the GDPR); *see also* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 18, 37–44 (2018) (providing an overview of CCPA). CCPA enters into effect in January 2020 and is considered a “mini GDPR regime” to the extent it seeks to grant users more control in their data and limits the collection and usage of data by corporations, as well as to equip regulators (and users) with more powerful remedies in the case of an abuse.

28. For example, Bakos et al. studied the browsing behavior of 48,154 consumers of ninety online software companies’ websites and found that 0.08% of consumers visited the EULA page of the software retailers and 0.22% of consumers visited the freeware companies’ EULA pages. *See* Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts*, 43 J. LEGAL STUD. 1, 19 (2014); *see also* Motion of Consumers Union and Public Knowledge for Leave to File Brief of *Amici Curiae* in Support of Defendants-Appellants at 1, *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005) (explaining that “every day consumers sign away important public rights as they rip and click through one-sided, non-negotiated shrink- and click-wrap contracts” and the public policy considerations underpinning such waivers).

29. Bakos et al., *supra* note 28, at 1, 19. Nevertheless, courts have generally enforced clickwrap agreements as long as the users had ample opportunity to read them and the contract is clearly presented. *See* *Hancock v. AT&T Co.*, 701 F.3d 1248, 1256 (10th Cir. 2012) (“Courts evaluate whether a clickwrap agreement’s terms were clearly presented to the consumer, the consumer had an opportunity to read the agreement, and the consumer manifested an unambiguous acceptance of the terms.”); *see also* *Specht v. Netscape Comm’ns Corp.*, 306 F.3d 17, 32–35 (2d Cir. 2002); *Serrano v. Cablevision Sys. Corp.*, 863 F. Supp. 2d 157, 164 (E.D.N.Y. 2012). The Restatement reporters conducted a comprehensive empirical study

agreements—a part of a vertical boilerplate³⁰ to which future creators and innovators are forced to agree as a pre-condition to their academic studies or employment.³¹ Empirical research supports the proposition that “I accept” is, in fact, the biggest lie of the information age, showing that the absolute majority of users will go as far as assigning their first-born child to sign in and gain access to a fictitious social network.³² And although form contracts and licenses are the lifeblood of any economy, especially that of instant “click-based” consumption of digital innovations and cultural assets, “[the] benefits of standard form contracting are not without risks.”³³ In other words, with great contracting power comes greater social responsibility.³⁴

finding ninety-two cases in which clickwrap contracts were enforced, in both federal and state courts. *See* RESTATEMENT OF THE LAW CONSUMER CONTRACTS, COUNCIL DRAFT NO. 5 at 46 (AM. LAW INST. 2018) [hereinafter *The Restatement*], https://www.ali.org/media/filer_public/05/30/053007a1-2b37-4142-b9c3-7a881e847d50/consumer_contracts_-_td_-_online.pdf [<https://perma.cc/U8DK-G4CH>]. Recently in a notable case in California, discussing the distinction between browsewrap and clickwraps when it comes to contract enforceability and formation, one court enforced a browsewrap contract that “prominently informed [users] on at least two occasions prior [to the purchase]” since they clicked “Accept and Continue” or “Sign In,” and after that “Submit Order” and therefore they agreed to the ToS, “which were always hyperlinked and available for review.” *See* *Nevarez v. Forty Niners Football Co.*, No. 16-CV-07013, 2017 U.S. Dist. LEXIS 131208, *20–22 (N.D. Cal. Aug. 15, 2017). The Restatement seems to focus on the conditions of the formation of the contract and not necessarily its type. *See* *The Restatement*, at 42. This approach is in line with the technological developments brought about with the age of connected devices, where consent will be obtained in a variety of novel ways via untraditional procedures, screens, and devices.

30. The fact that IP boilerplate contracts often accompany other contracts is problematic and affects the information costs imposed on adherents. *See* James Gibson, *Vertical Boilerplate*, 70 WASH. & LEE L. REV. 161 (2013) (performing a vertical study of boilerplate in consumer transactions in order to examine the information burden throughout the full transactional process, and finding that a computer purchase involves between 12 to 27 contracts, with a total word count ranging from 33,128 to 96,641 words, respectively). If in the “real-world” “transactions often involve multiple layers of contracts, each with its own information costs,” then in the connected world, in which adding another layer of information is nearly costless for the drafter, the problem is more severe. *Id.*

31. *See Bezalet's Policy*, *supra* note 9; Steven Cherenksy, *A Penny for Their Thoughts: Employee-Inventors, Preinvention Assignment Agreements, Property, and Personhood*, 81 CALIF. L. REV. 595, 595 (1993).

32. *See* Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 2018 INFO., COMM. & SOC'Y 1, 16 (noting that of more than 500 surveyed users, ninety-three percent accepted a “first-born child” assignment term and ninety-eight percent failed to spot (missed) the term in the ToS).

33. *The Restatement*, *supra* note 29, at 1.

34. Boilerplate, and even technological boilerplate, does not just operate as a negative force in IP property and creative regimes. First, it is important to recognize that contracts, including and especially standardized ones, serve a critical function in the IP realm; they

While the problem of IP boilerplate and private ordering is not new to the IP discourse, solutions are wanting. IP scholars often reject general contract doctrines as ill-equipped, favoring ad hoc retrofitted doctrines and legislative solutions. Contracts scholars tend to discard IP considerations, thus perpetuating consumerist perspectives. Consumer-focused doctrines have yet to adequately accommodate the needs of the “new” consumers, who pay with data and IP rights for “free services.”³⁵ The preemption doctrine, which was supposed to be the main mechanism for policing boilerplate that undermined federal IP policies, at least in the copyright context, proved to be a double-edged sword in the aftermath of *ProCD*, a notable case deciding that contractual expansions of copyright protections or scope in standard-form contract settings, enforced by state law, do not preempt federal law. If the contractual provision is not preempted by federal IP law, which is usually the case,³⁶ the question of enforceability is left solely to contract laws, where

facilitate transactions and allow innovations and cultural products to be disseminated and commodified. Licensees are the lifeblood of digital (and tangible) technology, and as such they (and the rights they facilitate) are praised by scholarship and protected by courts. See Merges, *Intellectual Property and the Costs of Commercial Exchange*, *infra* note 52; see also Merges, *The End of Friction? Property Rights and Contract in the Newtonian World of On-Line Commerce*, *infra* note 52. In as much as form contracts are critical to any industry, they are vital in a digital world of instant, “click-based” consumption. See Reichman & Franklin, *infra* note 106, at 876–78. But beyond that, boilerplate language could be used to foster innovation and creativity by displacing, at scale, IP laws’ default restrictive regime (of all rights reserved) with a more flexible (some rights or no rights reserved) regime that supports secondary creativity, commentary, access, and interoperability. The notable examples in this regard are Creative Commons licenses and Open Source licensing. See Shaffer Van Houweling, *Author Autonomy and Atomism in Copyright Law*, *infra* note 58; see also Menell, *Economic Analysis of Network Effects*, *infra* note 116, at 32; ERIC VON HIPPEL, *DEMOCRATIZING INNOVATION* (2005) and STEVEN WEBER, *THE SUCCESS OF OPEN SOURCE* 213 (2004). In the context of security research, boilerplate contracts can be used to introduce protections from anti-hacking laws and foster research, while the legal landscape continues to be murky. See Amit Elazari Bar On, *Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties*, in *REWired: CYBERSECURITY GOVERNANCE* (Ryan Ellis & Vivek Mohan Eds. 2019).

35. See *infra* note 352.

36. Professor Guy Rub recently conducted a comprehensive review of 288 court decisions that analyzed the application of copyright preemption and reached the conclusion that U.S. law broadly adopted the “No-Preemption Approach,” associated with the *ProCD* decision. Under this approach, boilerplate, as contracts, are not preempted by copyright law (17 U.S.C. § 301(a)) by definition, regardless of the content of the provision, since contractual rights are rights in personam, not equivalent to copyrights, which are rights in rem, and they require the proof of one “extra element” to institute a claim—the contractual promise. Guy A. Rub, *Copyright Survives: Rethinking the Copyright-Contracts Conflict*, 103 VA. L. REV. 1141, 1164–67 (2017) [hereinafter Rub, *Copyright Survives*]. Rub found that the “the no-preemption approach is currently the dominant one,” and that “[t]he Sixth Circuit is the only federal appellate court in the last twenty years to find a contract actually preempted by the Copyright Act.” *Id.* at 1170, 1180.

currently little, if any, attention is given to promoting the purposes of IP policies. Indeed, preemption has long deviated from its original purpose and has been reduced, as some claim, to “mechanically applying tests that, too often, have little to do with identifiable federal copyright policies.”³⁷

The result is that under U.S. law, private entities, acting as legislatures,³⁸ are allowed to undermine IP policies prescribed by federal IP laws through the use of boilerplate, an action that even state legislatures are prohibited from taking.³⁹ The same pattern of democratic degradation persists in data protection and privacy, where decades-long research has demonstrated the inability of consumers to comprehend lengthy privacy policies or notices and how this inability affects market competition over the quality of privacy-related contractual clauses.⁴⁰

Meanwhile, the role of private ordering in IP is gradually expanding and the U.S. standard form contracts body of law remains incoherent and unsettled.⁴¹ As society shifts from the production of physical commodities to

37. Guy A. Rub, *A Less-Formalistic Copyright Preemption*, 24 J. INTELL. PROP. L. 327, 330 (2017), [hereinafter Rub, *A Less-Formalistic Copyright Preemption*].

38. RADIN, *supra* note 1, at 16, 213 (explaining how boilerplate, in general, and specifically in the case of IP, are acts of democratic degradation; they employ mass systems of contracts to restructure and supersede the rights given by legislators, taking away rights granted by the democratic process); *see also* Kessler, *supra* note 4.

39. Under the copyright doctrine of preemption, and the doctrine of Supremacy Clause preemption. *See generally* Goldstein v. Cal., 412 U.S. 546, 562 (1973) (citing Hines v. Davidowitz, 312 U.S. 52, 67 (1941)) (explaining that the core concern under the Supremacy Clause preemption inquiry is to establish whether a state statute “stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress”). In the context of patents, *see* Bonito Boats v. Thunder Craft Boats, 489 U.S. 141, 160–61 (1989) (voiding a Florida statute as conflicting with federal patent law under the Supremacy Clause of the U.S. Constitution since it prohibited “the entire public from engaging in a form of reverse engineering of a product in the public domain . . . and substantially [restricted] the public’s ability to exploit ideas that the patent system mandates shall be free for all to use”); Rub, *A Less-Formalistic Copyright Preemption*, *supra* note 37, at 329; *cf.* Bowers v. Baystate Techs., 320 F.3d 1317 (Fed. Cir. 2003); Davidson & Assocs. v. Jung, 422 F.3d 630, 639 (8th Cir. 2005) (illustrating how the court did not find copyright preemption in a case where the drafter prohibited users from reverse engineering, a conduct that is permitted under fair use).

40. *See, e.g.*, Nathaniel Good et al., *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, 2005 ASS’N COMPUTING MACHINERY: PROC. SYMP. ON USABLE PRIVACY & SECURITY 43; Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3.1 IEEE SECURITY & PRIVACY 26 (2005) (providing survey evidence as to how the bounded rationality of users affects their privacy decision-making processes and attitudes).

41. In 1983, Rakoff noted that “the law currently governing contracts of adhesion is a jumble of different lines of analysis, contradictory outcomes, and convoluted expressions.” Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173, 1197 (1983). This proposition was repeated by other scholars throughout the years, including in IP

the creation of intellectual goods and advances in technology, and everything becomes interconnected,⁴² both the complexity and the variety of procedures governed under private ordering in IP settings are increasing. Private ordering is affecting other areas of technology law like security, algorithmic auditing, and privacy-enhancing research.

Every day, proprietors devise innovative ways to commercialize the intangibles created by others, and the means allowing them to do so are often newly drafted contractual terms. Legislators are not able to address these developments in an efficient, coherent, and timely manner, and their failure creates the legal environment in which abusive private ordering prospers. Furthermore, courts continue to struggle to address unique problems presented by non-negotiated contracts with ill-equipped binary tools, such as preemption, misuse, and exhaustion, which do not allow contextualization according to the type of contract in place. In their despair, some courts turn to copyright and patent misuse, which are “capture-all” doctrines that are now being redesigned to address a variety of policy concerns. However, these are not specifically tailored to mass-market consumer contracts, nor do they provide a firmer ground or certainty.⁴³

Misuse, an equitable doctrine originating from the “unclean hands” doctrine, is a form of defense that is focused on anti-competitive or otherwise abusive behavior of the drafter that seeks to expand its monopolistic control.⁴⁴

contexts. See Tom W. Bell, *Fair Use v. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557, 607 (1998).

42. This “disruptive technological revolution” is commonly referred to as the “Internet of Things,” where the “Internet [is able] to reach out into the real world of physical objects.” Mohamed Ali Feki et al., *The Internet of Things: The Next Technological Revolution*, 46.2 COMPUTER 24 (2013). As connected devices operate on licensed software, this revolution also affects the proliferation of the IP boilerplate and introduces new challenges.

43. Nonetheless, some scholars resorted to these doctrines as a primary solution. See, e.g., Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CALIF. L. REV. 111, 157–58 (1999) [hereinafter Lemley, *Beyond Preemption*] (“Furthermore, because copyright misuse is a fact-specific doctrine tailored to the circumstances of individual cases, it may prove a better tool both for tailoring copyright incentives and for avoiding the reticence that surrounds coarser tools such as preemption.”). Others were less optimistic, noting that misuse “is primarily directed at combating particularly egregious contracts” and is ill-equipped to address such a “diffused” and widespread problem. See Viva R. Moffat, *Super-Copyright: Contracts, Preemption, and the Structure of Copyright Policymaking*, 41 U.C. DAVIS L. REV. 45, 103 n.257 (2007).

44. See generally Brett Frischmann & Dan Moylan, *The Evolving Common Law Doctrine of Copyright Misuse: A Unified Theory and Its Application to Software*, 15 BERKELEY TECH. L.J. 865, 867–70 (2000) (explaining that misuse operates as a defense and is focused on antitrust principles, although there are instances where general public policy considerations are considered, as well); see also *Assessment Techs. of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640, 647 (7th Cir. 2003) (applying copyright misuse “beyond the bounds of antitrust” in a case in

IP misuse prevents copyright and patent holders “from leveraging their limited monopoly to allow them control of areas outside the monopoly.”⁴⁵ While Unconscionability 2.0 serves as a proposed solution applicable to all IP boilerplate types and is particularly well suited for the adherent-creator type of contract, misuse, as explained, can also operate as a partial solution in the case of the adherent-creator type of contract.⁴⁶

As the interface between contract and IP continues to grow, and the use of IP boilerplate that undermines IP policies prevails, several critical questions arise: Can contractual concepts accommodate IP notions? Can the normative origins of unconscionability facilitate reinterpretations reconciling freedom of contract with IP policies? Can U.S. law adopt an IP contract’s *lex specialis* in order to address the problems created by the IP boilerplate in a contextualized manner?⁴⁷ I claim that since the primary purpose of this emerging type of boilerplate is, in fact, to regulate innovations, U.S. law simply cannot continue to maintain the “ideological dissolution” between contract and IP law.⁴⁸ I

which an owner pursues an infringement suit “to obtain property protection . . . that copyright law clearly does not confer”); *Lasercomb Am., Inc. v. Reynolds*, 911 F.2d 970, 978 (4th Cir. 1990) (explaining that “[t]he question is not whether the copyright is being used in a manner violative of antitrust law . . . but whether the copyright is being used in a manner violative of the public policy embodied in the grant of a copyright”); *Disney Enters. v. Redbox Automated Retail, LLC*, No. CV 17-08655 DDP (AGRx), 2018 U.S. Dist. LEXIS 69103, at *17–18 (C.D. Cal. Feb. 20, 2018) (citing *Omega S.A. v. Costco Wholesale Corp.*, 776 F.3d 692, 699–700 (9th Cir. 2015)) (clarifying that “copyright misuse need not even be grounded in anti-competitive behavior, and extends to any situation implicating ‘the public policy embodied in the grant of a copyright’ ”); *infra* notes 190–203 and accompanying text.

45. *A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1026 (9th Cir. 2001).

46. Indeed, some scholars have proposed this doctrine as a solution to clauses that prohibit otherwise lawful reverse engineering or fair use. See Frischmann & Moylan, *supra* note 44, at 928 n.163; see also Lydia Pallas Loren, *Slaying the Leather-Winged Demons in the Night: Reforming Copyright Owner Contracting with Clickwrap Misuse*, 30 OHIO N.U. L. REV. 495 (2004) (suggesting that a broad public policy-based doctrine of copyright misuse, coupled with rebuttable presumption of misuse, could serve as a solution to cases in which copyright owners use contracts “to avoid the express statutory limitations on their rights”).

47. Cf. Giuseppina D’Agostino, *Contract lex rex: Towards copyright contract’s lex specialis*, in INTELLECTUAL PROPERTY AND GENERAL LEGAL PRINCIPLES: IS IP A LEX SPECIALIS? 4 (Graeme B. Dinwoodie ed., 2015) (articulating the concept of “copyright-contract *lex specialis*,” and claiming that there is “a need for a more copyright-contract-centric *lex*” and that “contract law should be more fully integrated into copyright in order to adequately serve the aims of copyright law”).

48. ABRAHAM DRASSINOWER, WHAT’S WRONG WITH COPYING? 202 (2015) (suggesting that in order to avoid such ideological dissolution between juridical orders, in instances where copyright claims encounter claims recognized in other juridical orders such as contract law, the law is required to mediate between competing claims through a structure of “proportionality” and “translation tools”); see also Amit Elazari Bar On, *Copyright and the Greater System of Rights: Utilizing Contractual Concepts to Solve Intellectual Property Problems in Standard-Form*

further claim that the unique problems presented by the intersection between standard form contracts and IP law should be solved by a tool that is informed by both disciplines. Introducing: Unconscionability 2.0, an inter-doctrinal solution.

Unconscionability is the prominent doctrine used to perform judicial scrutiny of boilerplate contracts. If a court deems a contractual term unconscionable, it could refuse to enforce it.⁴⁹ While most IP scholars discarded this doctrine as ill-equipped, my analysis, informed by comparative insights from Israeli jurisprudence, suggests that it is a viable solution that can accommodate extra-contractual notions. This view is also supported by the newly proposed Restatement of Consumer Contracts,⁵⁰ which as I explain, reformulates unconscionability to some extent and untangles it from its stringent, procedural routes.

Under the proposed solution, Unconscionability 2.0, the critical question of unconscionability should be examined by asking, substantially, whether the term benefits the purposes of the relevant IP policies or negates them. Most importantly, this solution allows courts to consider both IP and contractual considerations under the same doctrine, considering, *inter alia*, the salience of the term under the procedural analysis as well as externalities imposed on the public domain, and the displacement of IP policies under the substantive analysis. These considerations are then balanced under unconscionability's sliding scale approach, which allows the courts to reach one result for a negotiated contract and another in the context of boilerplate. It is a contextual tool, based on a case-by-case analysis of contract enforcement coupled with general presumptions of unconscionability, as opposed to the "all-or-nothing," categorical approach to IP boilerplate enforcement that is currently the solution under the prevailing interpretation of preemption.⁵¹ In IP terms, Unconscionability 2.0 allows courts to conduct a form of an implied conflict preemption analysis under the substantive unconscionability prong, and void

Contracts, 29 INTELL. PROP. L.J. 83 (2016) (elaborating how Unconscionability 2.0 fits into Drassinower's argument).

49. The Restatement, *supra* note 29; U.C.C. § 2-302; RESTATEMENT (SECOND) OF CONTRACTS § 208 (AM. LAW INST. 1981).

50. The Restatement, *supra* note 29, at § 5.

51. Rub, *Copyright Survives*, *supra* note 36, at 1144, 1171 (Surveying 279 cases and proposing the "no-preemption" approach is the prevalent interpretation for copyright preemption in the United States); *cf.* Pamela Samuelson, *Possible Futures of Fair Use Symposium*, 90 WASH. L. REV. 815, 859–60 (2015) (noting that an "articulation of standards for determining under what circumstances fair use should override license or technical restrictions" might evolve, that "[i]t seems unlikely that courts would accept that fair use should either always or never override contractual restrictions" and that "[t]he most promising approach is one that would override mass-market license restrictions that interfere with copyright policy purposes").

terms specifically in cases involving IP boilerplate that amounts to “private IP legislation,” under unconscionability’s nonsalience procedural analysis.⁵²

Drawing on moral foundations, this solution seeks to avoid utilitarian biases, invites discourse between competing theoretical approaches, and facilitates “foundational pluralism.”⁵³ As a legal standard applicable to diverse contractual relationships, even those that are non-consumer-based, it accommodates the dynamic adjustments often required when IP policies seek to address contemporary problems. Indeed, this is a tool that applies to all adherents, including users of free products and businesses. Unconscionability 2.0 is one way an IP regime can operate within an existing contractual doctrine, and how one framework can involve both contractual and IP considerations.

It is precisely because the doctrine is deeply rooted in contract law that its flexibility and broad applicability could well serve as a universal solution to myriad problems created by appropriating contracts. Yet Unconscionability 2.0 cannot operate in a vacuum. While this suggested interpretation requires just one bold U.S. court for its adoption,⁵⁴ and no legislative reform, other solutions I propose, some based on Israeli standard form contract law, will require broader legislative efforts.⁵⁵ I further explain how this type of solution

52. See Robert P. Merges, *The End of Friction? Property Rights and Contract in the Newtonian World of On-Line Commerce*, 12 BERKELEY TECH. L.J. 115, 126 (1997) (“[A] dominant contractual form can operate as a form of ‘private legislation’ that restricts federally conferred rights every bit as much as a state statute.”). Indeed, Unconscionability 2.0 is a new tool to achieve what Professor Merges suggested twenty years ago: a “new doctrine of contract preemption [that] would apply only when the contract term rises to the level of private legislation.” Robert P. Merges, *Intellectual Property and the Costs of Commercial Exchange: A Review Essay*, 93 MICH. L. REV. 1570, 1613 (1995); cf. Rub, *A Less-Formalistic Copyright Preemption*, *supra* note 37, at 327 (claiming that under its current interpretation, preemption has failed to serve its function and “calling courts to routinely apply the principles of implied preemption when state law seems to conflict with or to stand as an obstacle to federal copyright policy”).

53. See Robert P. Merges, *Against Utilitarian Fundamentalism*, 90 ST. JOHN’S L. REV. 681 (2016) [hereinafter Merges, *Against Utilitarian Fundamentalism*] (discussing the importance of foundational pluralism in the conceptualization of IP regimes). Unconscionability 2.0 can facilitate such pluralism by focusing on the midlevel principles: proportionality, efficiency, nonremoval of the public domain, and dignity, that provide “common conceptual vocabulary for conducting policy debates” in IP. These principles “create an overlapping consensus among people with differing beliefs about the ultimate normative foundations of IP law.” *Id.* at 702–03.

54. See I.C. *ex rel.* Solovsky v. Delta Galil USA, 135 F. Supp. 3d 196 (S.D.N.Y. 2015); *infra* note 265.

55. While Unconscionability 2.0 confers discretion upon courts, it is still an intermediary approach since it allows them to partially enforce or amend clauses. Radin, in contrast, on at least one occasion suggests that boilerplate “should be declared invalid in toto, and recipients should instead be governed by the background legal default rules,” because “it [is] much harder for courts to sever and excise only certain clauses.” RADIN, *supra* note 1, at 213. Yet as she clarifies, this reference applies only to “‘offending’ boilerplate—meaning mass-market

can operate in some case studies, including the case of the student-creator. I lay a vision for Unconscionability 2.0, with application in various settings, from negotiated contracts to “technological boilerplate,” and cases of boilerplate language interacting with cybersecurity or algorithmic decision-making considerations.

The Article proceeds as follows: the second Part focuses, in a nutshell, on the problem. It introduces the phenomenon of the IP boilerplate and the manner in which such boilerplate undermines IP policies, as part of the more general process of privatization of IP regulation as consumer culture changes and technology evolves. One potential reason why unconscionability has been underutilized in U.S. IP law is that the doctrine has been sporadically discussed only in reference to selected types of contracts, alongside other solutions. Generally, the literature lacks a unified discussion of IP boilerplate,⁵⁶ yet such a comprehensive account is not the purpose of this Article, which focuses instead on the solution. Still, this Part aims to provide the reader with an understanding of why IP boilerplate poses a unique normative challenge that merits a unique solution. It further suggests a new paradigm to observe the IP boilerplate problem: a distinction between adherent-user and adherent-creator types of contracts.

Adherent-creator contracts are IP boilerplate contracts in which the adherent—the one who does not read the fine print and lacks bargaining power—is the original owner of the IP rights.⁵⁷ The drafter owns nothing, yet seeks to assign or regulate the rights of the adherent in his creations. These contracts have received less attention in IP scholarship than EULAs, in which the drafter owns the IP. Nevertheless, in this highly technologically connected

boilerplate that is bad enough to incur tort liability for intentional deprivation of core legal rights.” See Margaret Jane Radin, *What Boilerplate Said: A Response to Omri Ben-Shabar (and a Diagnosis)*, L. & ECON. WORKING PAPERS no. 98, 3 n.7 (2014), https://repository.law.umich.edu/law_econ_current/98/ [https://perma.cc/9LZD-JHUM] [hereinafter Radin, *What Boilerplate Said*]. Arguably, the Israeli experience shows that courts can in fact police unconscionable terms efficiently.

56. Scholarship, ever addressing the problems created by reality, has evolved step-by-step, usually focused on one or another strain of IP boilerplate. See, e.g., Cherenky, *supra* note 31 (discussing whether a contract was a pre-invention assignment contract signed by employees); Lemley, *Shrinkwrap Licenses*, *supra* note 23 (analyzing a shrinkwrap license seeking to limit the rights of the end user); Sandip H. Patel, *Graduate Students’ Ownership and Attribution Rights in Intellectual Property*, 71 IND. L.J. 481 (1996) (discussing an academic institution’s IP policy depriving students of rights in their creations). This has resulted, as claimed, in a scholarly literature that discusses only a part of the contracts, and therefore, often, only a part of the relevant purposes of IP law.

57. In contrast, adherent-user types of contracts are IP boilerplate in which the offeror is both the creator and drafter of the contract, thereby enjoying supremacy in information and bargaining power, while the adherent is the user.

era, non-drafters are producing more innovations, and therefore these contracts are on the rise. While we often speak of the age of “user-generated content,”⁵⁸ it might be more worthwhile to discuss “adherent-generated content,” as this recent expansion mandates theoretical adaptations from both an IP and standard form contract perspective. This Part also briefly addresses the chief solutions that are currently used by courts and legislators to address the problems created by IP boilerplate, such as preemption, misuse, and ad-hoc legislative solutions. It further discusses some positive IP boilerplate that fosters creativity as well as the rise of some less positive technological IP boilerplate that may give rise to “unconscionability by design.” Finally, this Part describes the overall emerging narrative of the “game of catch” IP regulation has been playing with IP boilerplate, one in which the latter still seems to be winning.

The third Part focuses on the current underutilization of unconscionability in the United States as a solution to the problems discussed in the second Part. While courts in other jurisdictions, specifically Israel, have used unconscionability to prevent drafters from undermining IP policies, U.S. courts have not. Instead, U.S. courts have resorted to the doctrine of preemption. But in the aftermath of *ProCD*, preemption has not only failed to solve the problem but has cultivated the ideological dissolution between U.S. contract laws (on the state level) and IP laws (on the federal level). This created a legal reality in which contractual doctrines are, by definition, uninformed by IP policies, even if the sole purpose of the contract is regulating IP rights. The third Part further presents and critiques this underutilization of unconscionability in U.S. law. It exposes a long-dominating, yet unobserved narrative of an alienating discourse between IP and contracts regimes in the United States, one that applies in the context of first-sale and exhaustion cases well. It also discusses how courts resorted to misuse and first-sale in recent IP boilerplate cases, and how these doctrines fail to fully address boilerplate

58. In Samuelson’s terms: “Never before in human history has it been more possible for tens of millions of people around the world to express themselves in creative ways, including by tinkering with existing artifacts and sharing the fruits of their creativity with others.” Pamela Samuelson, *Freedom to Tinker*, 17 THEORETICAL INQUIRIES L. 563, 564 (2016) [hereinafter Samuelson, *Freedom to Tinker*]; see also Peter S. Menell, *This American Copyright Life: Reflections on Re-Equilibrating Copyright for the Internet Age*, 61 J. COPYRIGHT SOC’Y U.S.A. 235, 347 (2014) (noting that “[d]igital technology has empowered anyone to remix art and the Internet has opened vast content distribution channels. Creators no longer need to go through traditional professional gatekeepers — publishers, studios, broadcasters, and record labels. They can reach a massive audience through all manner of user-generated content websites”); Molly Shaffer Van Houweling, *Author Autonomy and Atomism in Copyright Law*, 96 VA. L. REV. 549, 552 (2010) (“Technologically empowered individual creators are thus potential casualties of a regulatory regime that propertizes the ingredients of iterative creativity, but they are also among the beneficiaries of copyright law’s largess.”).

issues.

The fourth Part focuses on the solution, Unconscionability 2.0. It aims to resurrect unconscionability as a pragmatic solution and is informed by comparative analysis, particularly Israeli jurisprudence's purposeful approach to the doctrine. This Part briefly presents the Israeli purposive approach to unconscionability and the manner in which Israeli case law has utilized unconscionability to solve problems created by IP boilerplate. It discusses the proposed doctrine of Unconscionability 2.0 and its advantages, and its potential application in U.S. law. It lays a more robust vision for Unconscionability 2.0, and suggests mechanisms to increase clarity and certainty, such as presumptions of unconscionability. It further applies Unconscionability 2.0 to technological boilerplate in negotiated contracts and demonstrates how Unconscionability 2.0 could be applied in various case studies, including the case of the student-creator. The Part concludes by addressing some critiques of Unconscionability 2.0. The conclusion follows.

II. INTRODUCING IP BOILERPLATE: WHEN THE FINE PRINT UNDERMINES CREATIVITY AND INNOVATION

Boilerplate contracts are not a new societal phenomenon. In fact, humans, not just consumers, have been subjected to unilateral “take-it-or-leave-it” contracts since the invention of contracts as a legal institution more generally around the sixteenth century.⁵⁹ As time passed, and the need to facilitate transactions between large populations emerged with the advent of mass production,⁶⁰ the notion of “Freedom of Contract” developed hand-in-hand with its “nemesis” counterpart—unnegotiated standard form contracts, drafted by one but offered to many: many that ought to accept and have no negotiating power (or information). These contracts are otherwise known as “contracts of adhesion.”⁶¹ As such, form contracts have been thoroughly investigated by legal scholarship for centuries, with early scholarship tracing back to the first

59. A.W.B. Simpson, *The Hornvitz Thesis and the History of Contracts*, 46 CHI. L. REV. 533, 543 (1979) (explaining that “[i]t was settled in the sixteenth century that mutual promises could be consideration for each other” and providing an historical account of contract law theory).

60. The development of standard form contracts as a transactional tool is often associated with the industrial revolution and the growing need to facilitate and scale commercial transactions that came about with the advent of the mass-production era. *See* Slawson, *supra* note 17, at 530.

61. A term coined by Patterson in the course of discussing life insurance boilerplate. *See* Edwin W. Patterson, *The Delivery of a Life Insurance Policy*, 33 HARV. L. REV. 198, 222 (1919) (“Furthermore, ‘freedom of contract’ rarely exists in these cases. Life-insurance contracts are contracts of ‘adhesion.’ The contract is drawn up by the insurer and the insured, who merely ‘adheres’ to it, has little choice as to its terms.”).

decades of the twentieth century.⁶²

In 1943, Kessler characterized this unique type of contract as “private law,” contracts that “[enable] enterprisers . . . to legislate in a substantially authoritarian manner without using the appearance of authoritarian forms,” thereby “impos[ing] a new feudal order of their own making upon a vast host of vassals.”⁶³ He was the first to distinguish between contracts, a legal tool that was perceived at the time as “a private affair and not a social institution,”⁶⁴ and form contracts that amount to a “living law,” a vessel to empower “industrial empires”⁶⁵ that must be kept in check as a threat to democratic systems, especially in the hands of monopolistic entities.⁶⁶

This analytic framework for exploring the problematic nature of form contracts was later developed by Slawson in his seminal 1971 paper. Slawson explained that by virtue of their dominance in the market, form contracts became a de facto meaningful part of the applied body of law, but one that is not subjected to the same stringent requirements required from formal legislation in a well-functioning democratic society.⁶⁷ His suggestion, decades ago, was that if contracts of adhesion do not rely on the meaningful consent of both private parties—one that is usually provided by democratic processes—the legitimacy of form contracts’ content must stem from another source: whether they reflect standards that comply with the public interest.⁶⁸ It is this conformity with “higher public laws” that allows privately-made law to legitimately “govern the public” as an alternative, private mode of legislation. To effectively subject form contracts to this type of judicial review, “an

62. See Karl N. Llewellyn, *What Price Contract—An Essay in Perspective*, 40 YALE L.J. 704 (1931); Issacs, *The Standardizing of Contracts*, 27 YALE L.J. 34 (1917); see also K.N. Llewellyn, *Book Review*, 52 HARV. L. REV. 700 (1939) (reviewing OTTO PRAUSNITZ, *THE STANDARDIZATION OF COMMERCIAL CONTRACTS IN ENGLISH AND CONTINENTAL LAW* (London, Sweet & Maxwell, 1937)).

63. See Kessler, *supra* note 4, at 640 (coining the term “legislation by contract”); see also Robert P. Merges, *Intellectual Property and the Costs of Commercial Exchange*, *supra* note 52, at 1611–14 (discussing contracts as “private legislation” and applying Kessler’s argument to shrinkwraps, claiming “they have the same effect as offending state legislation”).

64. Kessler, *supra* note 4, at 630.

65. *Id.* at 632.

66. *Id.* at 641–42.

67. Slawson, *supra* note 17, at 535–37.

68. *Id.* at 566. Such “non-authoritative standards” encompass the “reasons, principles, or considerations possessing no legal authority within the jurisdiction but of greater generality than the law being reviewed and serving to demonstrate that it is in the public interest.” *Id.* at 533, 538–39.

‘administrative law’ of contracts”⁶⁹ must be developed.⁷⁰

Building on Slawson’s argument, Rakoff asserted that because of the nature of form contracts, “a different body of law” is needed to address the question of enforceability.⁷¹ For Rakoff, the adherent aspect of the drafting process should be the focus of the inquiry, rather than the presence of monopoly or preexisting market power. Contracts with an absent adherent are contracts of adhesion. The “invisible” terms contained in such a contract—the terms that go beyond the contents of “ordinary contracts,” such as the price—are presumptively unenforceable,⁷² and judges would therefore need to apply the “background law” to establish the result. The legal system therefore needs to develop the body of terms that is best fitting to each and every transaction—a challenging, and costly, task.⁷³ In 2003, Korobkin added another fundamental piece to the standard form contract enforcement debate, suggesting that the focal point of the analysis should rest on the notion of the contractual terms’ “salience,” a term that would fifteen years later become the cornerstone of unconscionability analysis in the proposed Restatement.

According to Korobkin, buyers are “boundedly rational decisionmakers,”⁷⁴ and therefore their ability to price contractual terms in their entirety is limited. They simply do not have the economic incentive to invest the time required to understand and evaluate all of the contract’s terms. Because a market does not form to police the quality of these potentially “socially inefficient” terms, these “nonsalient” terms, which are not evaluated by a significant number of buyers, must be subjected to judicial review. By adapting the procedural prong of the unconscionability test to address the question of salience, and spotting cases in which a significant number of buyers are rationally bounded, courts will be able to distinguish efficient terms from inefficient terms. Nonsalient terms should be evaluated with suspicion and policed *ex post*. Meanwhile, *ex ante* legislation should provide mandatory alternative terms that reflect socially desired, efficient results.⁷⁵

69. *Id.* at 533.

70. As I will explore, that same principle is exhibited in the Israeli purposeful approach to unconscionability, which brings forth, under a specific law, a unique judicial review process to form contracts conducted by a designated tribunal.

71. Rakoff, *supra* note 41, at 1175.

72. *Id.* at 1251; *see also* Llewellyn, *Book Review*, *supra* note 62, at 704 (arguing that if the form terms are unreasonable, they should not be enforced).

73. Rakoff, *supra* note 41, at 1258–59.

74. Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1204–06 (2003). In fact, it is because of the bounded rationality of consumers that the “market will often include terms that are socially inefficient, leav[ing] buyers as a class worse off.” *Id.* at 1206.

75. *Id.* This type of framework is provided by the U.C.C., for example.

Other scholars put forth a variety of alternative solutions to address the question of standard form contract enforceability, but with the advent of the information age and the introduction of cheap electronic contract formation, form contracts expanded to all of life's domains. Meanwhile, U.S. laws, and courts, struggle to develop a comprehensive, systemic regime to address the question of enforceability. In fact, as many scholars previously claimed, the digital revolution exacerbated the problem, as a new type of information feudalism emerged.⁷⁶

This Part focuses on one particular aspect of the skirmish: the interaction between form contracts and IP policies and some of the specific issues they create. A full account of these problems is beyond the scope of this Part. Yet this Part proposes a new analytical framework to explore the variety of interactions between IP and contracts, one that focuses on the distinction between the adherent-creator and the adherent-user. It will also bring forth some of the thorniest examples of problems created by IP boilerplate in both virtual and real-world creative platforms. It will make the case that IP boilerplate is unique and merits a unique solution. In a world governed by the “myth of free”⁷⁷ and social media platforms, creative content has become a commodity that users exchange for a variety of services. Meaningful innovations are created in collaborative, dialogical processes, bringing together creative minds from communities across territories. These innovations and creations and the processes that led to their creation are all governed by private rules, known as Terms of Service (ToS), ubiquitous to all websites and digital applications. The digital age changed the way we consume cultural assets and contribute to their creation. It also introduced a new type of form contract focused on the regulation of this unique mode of creation and consumption.

These form contracts contain IP boilerplate language and create unique challenges. Empirical evidence suggests IP boilerplate language regulating IP rights is especially nonsalient. Not only is there no competition over the quality of the terms in the market, but companies also offer very similar terms⁷⁸ and

76. See generally Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of “Rights Management”*, 97 MICH. L. REV. 462 (1998).

77. See *infra* note 352.

78. See, e.g., Alison C. Storella, *It's Selfie-Evident: Spectrums of Alienability and Copyrighted Content on Social Media*, 94 B.U. L. REV. 2045, 2064 (2014) (explaining that in social networks a phenomenon of “copycat boilerplate” persists, where the same licensing language is becoming “standard practice” that “makes it impossible for users to exit their contracts for more advantageous terms”); see also Casey Fiesler et al., *Reality and Perception of Copyright Terms of Service for Online Content Creation*, PROC. 19TH ACM CONF. ON COMPUTER-SUPPORTED COOPERATIVE WORK & SOC. COMPUTING 1450, 1453 (2016). The author's own coauthored research findings further suggest that very similar language exists in platforms' ToS, and

users and consumers find them especially confusing, in the rare cases that they read the terms. As such, IP boilerplate often exhibits severe societal externalities as it regulates cultural assets and the public access to innovation, as well as what remains in the public domain. These issues are explored in this Part. The first Section proposes a new analytical perspective to facilitate the discussion of IP boilerplate according to the *adherent-user* and *adherent-creator* distinction. The following Section demonstrates the variety and complexity of problems created by IP boilerplate.⁷⁹ Examples will encompass fair use waivers of different kinds, post-sale restrictions on how users can dispose of and use artifacts that embody patents or copyright, and various assignments of, and other limitations on, creators' and inventors' rights. This Section also exposes an interesting narrative: traditional solutions such as preemption and misuse are specifically ill-equipped to address problems created by adherent-creator types of IP boilerplate.

The next Section briefly discusses the rising phenomena of technological boilerplate, code that operates as boilerplate and enforces boilerplate. The following Section introduces, in a nutshell, the rising opposition to IP boilerplate: the use of private-ordering mechanisms meant to achieve the deproertization of the public domain or the flexible assignment of IP rights (e.g., Creative Commons licenses and the GPL open-source license).⁸⁰

further provides survey evidence that users' attitudes towards these terms do not change significantly across platforms. Amit Elazari Bar On et al., *infra* note 82.

79. See Rub, *Copyright Survives*, *supra* note 36, at 1149 (conducting a comprehensive review of court decisions that analyzed preemption to reach the conclusion that "the horror scenarios that envisioned contractual arrangements running wild and trumping copyright law as we know it have not materialized" and "[i]t is doubtful that contracts do, in fact, affect users' behavior in a way that disturbs the arrangements set by copyright law without leaving a trace, in the case law or elsewhere"). Yet Rub focused only on litigated cases which involved preemption (adherent-user types of contract), and the majority of the cases he examined did not involve boilerplate at all. *Id.* Interestingly, the most pressing and oppressive cases of adherent-creator types of contracts do not involve preemption at all. See, e.g., *Solovsky v. Delta Galil USA*, 135 F. Supp. 3d 196 (S.D.N.Y. 2015). Rub's research suggests there is a need to address the manner in which non-litigated IP boilerplate undermines copyright policies, and most importantly, to offer solutions that will reduce litigation barriers and increase judicial scrutiny of IP boilerplate, as this Article attempts. See Rub, *Copyright Survives*, *supra* note 36, at 1149.

80. See Molly Shaffer Van Houweling, *The New Servitudes*, 96 GEO. L.J. 885, 928–38 (2008) (describing such licenses that give users permission to perform what would be otherwise unlawful under copyright as "new servitudes"). These emerging servitudes do involve notice and information costs, but such costs are balanced against the fact that they regulate uses which are already governed by copyright law, as opposed to "behavior outside the scope of copyright law's exclusive rights." *Id.* at 937. In other words, compliance with general copyright law would have imposed similar "information-intensive investigation" as complying with such

A. THE ADHERENT-USER AND THE ADHERENT-CREATOR DISTINCTION

The term “adherent” developed within the standard form contract literature concurrently with the conceptualization of contracts of adhesion. An adherent, simply put, is the “non-drafter” of the agreement, the party to the form-agreement who agrees to the terms, and often lacks negotiation power or full information regarding the contractual terms and the transaction. It is the party that *adheres* to the contractual terms offered by the drafter. Whether the adherent ought to be a consumer, or a “buyer” that exchanges money for the transaction or services, so as to trigger the application of standard form contract law, depends on the jurisdiction. Israeli law defines the term “adherent” broadly to include essentially any non-drafter party, including employees, commercial parties and corporations, union members, and of course, users of free services.

According to the proposed distinction, adherent-creator contracts are IP boilerplate in which the adherent, the one who does not read the fine print and lacks bargaining power, is also the original owner of the IP rights: for example, the author of a creative work.⁸¹ The drafter owns nothing, yet seeks to assign or regulate the rights of the adherent in her creations. The most common example is social media platforms’ ToS, which will include copyright license language as to how the platform, and its affiliates, may use the content created by the adherent—the user of the platform, but also the creator of the original work. Can this content be “sublicensed” to other entities, or can the platform make commercial use of user-generated content?⁸² These are the rights regulated under this adherent-creator boilerplate. To clarify, although the adherent in our case is the user of the social media platform (thus, the commonly used term “user-generated content”), under this paradigm, she is an adherent-creator.

In contrast, adherent-user contracts are IP boilerplate in which the offeror is both the creator of the IP in the work or innovation and the drafter of the contract, thereby enjoying supremacy in information and bargaining power, while the adherent is the user of the work. The prominent example here is the “notorious” EULA, in which the drafter is the owner of copyright-protected software and the boilerplate is used to limit the contours of usage license given to an adherent as a user of the work. In patents and copyrights, EULAs can

licenses. *Id.* The costs associated with such positive IP boilerplate are also balanced against the positive externalities they impose. *Id.* at 949.

81. 17 U.S.C. § 201(a) (2018).

82. See Amit Elazari Bar On et al., *A Penny for Their Creations—An Empirical Study of Social Media User’s Awareness to Rights in Uploaded Creations* (forthcoming) (on file with author) (surveying different license terms of social media networks ToS and providing a detailed discussion).

also be used to impose restrictions on the manner in which the innovation is used, including circulation in secondary markets, a practice that was recently challenged in the Supreme Court. While, as I explain, it is this type of contract that has received most of the scholarly attention, in this highly technologically connected era, adherents are producing more creations and innovations,⁸³ and therefore adherent-creator contracts are on the rise.

But boilerplate has become a prominent tool to regulate creative processes beyond the common example of social media. Creative Commons licenses, for example, are standardized contracts that allow authors to license their work to users in more favorable terms than copyright law's default regime, and even to waive all rights in the creation and donate it to the public domain. Software code is created in cumulative open-source processes regulated by standardized contractual terms. And participants in creative communities like Wikipedia produce content under a set of standardized terms establishing their rights in the mutual product.⁸⁴

With the proliferation of IP boilerplate, this analytical framework distinguishing adherent-creators and adherent-users enables us to explore the problem from a nuanced standpoint. Both types of contracts can create externalities. EULAs are often characterized as containing overreaching terms that limit users' rights, most notably fair use. They thereby limit the public, and future creators and innovators, access to the creation beyond the careful balance prescribed by law. Adherent-creator contracts can affect the public domain differently, by depriving the original author of control and autonomy over the creation, stifling her future incentives to engage in creative work, and undermining the purposes of copyright protection. They can also create inefficient lock-ins on innovations by assigning works to the drafter, who is sometimes not better positioned to make the work accessible to the public,⁸⁵ or by limiting the circulation of the work in secondary markets.

From a consumer standpoint, the competition in the market over the quality of these terms (salience) is different, as is the level of consumers' (or users') knowledge of their fair use rights vis-à-vis ownership rights under the relevant IP mode. Users often lack understanding of both, but authorship or inventorship rights are uniquely complex and require further understanding of the monetary value of the work licensed, which is usually unknown at the

83. See, e.g., Shaffer Van Houweling, *Author Autonomy and Atomism in Copyright Law*, *supra* note 58.

84. See *About Wikipedia*, WIKIPEDIA <https://en.wikipedia.org/wiki/Wikipedia:About> [<https://perma.cc/AG9A-73GL>] (last visited Sept. 2, 2019). Wikipedia contributors are also subjected to social norms. See YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* (2006).

85. Leading Israeli design institutions broadly assign students' IP rights to the institution, although they rarely invoke their rights or commercialize the work or invention.

moment of contract formation. Fair use rights are also unpredictable to some extent, so they raise different concerns with respect to users' ability to evaluate them.⁸⁶

Research conducted by Hoofnagle and Perzanowski⁸⁷ showed that consumers lack an understanding of what they are buying when purchasing online digital media and the boundaries of ownership of such products versus contractual licensing. This includes which property restrictions are “attached” and apply to their use of the online product—restrictions that otherwise would not be applicable to the purchase of tangible cultural products like books and records under the first-sale doctrine.⁸⁸ Consumers, as the authors explain, are also subjected to “mixed signals” that lead them to believe they are actually “buying” the product as opposed to licensing it (with the most notable example being the “Buy Now” button on Amazon).⁸⁹ From an empirical standpoint, the authors found that among eighty-three percent of users who clicked a “Buy Now” button when purchasing a media product in the designed experiment believed they would own (as opposed to license) the digital good; that more than eighty-six percent of users believed they were entitled to keep the good bought forever, and that a large majority of users thought they could consume the media on any device they wanted to.⁹⁰ Sixteen percent of users thought they could resell the good.⁹¹

Thus, applying this distinction can lead to different results when reviewing IP boilerplate (when IP policies are grossly displaced); this is specifically because the creator of the work is the adherent, or in adherent-user IP boilerplate, since contractual rights may be less salient to users as opposed to creators. The distinction also serves to highlight the rise of adherent-creator contracts, and the scarcity of legal and empirical scholarship focusing on the emerging type of the adherent-creator boilerplate from an inter-doctrinal perspective.

At first blush, this distinction between adherent-users and adherent-creators of IP boilerplate seems straightforward. But some IP boilerplate, like social media platforms' ToS, combines both, regulating the license granted by

86. See, e.g., Matthew Sag, *Predicting Fair Use*, 73 OHIO ST. L.J. 47 (2012).

87. Aaron Perzanowski & Chris Jay Hoofnagle, *What We Buy When We Buy Now*, 165 U. PA. L. REV. 315 (2017); see AARON PERZANOWSKI & JASON SCHULTZ, *THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY* 83–101 (2016).

88. Consumers believe that when they “buy” digital media goods, they can “keep those goods permanently, lend them to friends and family, give them as gifts, leave them in their wills, resell them, and use them on their device of choice.” Perzanowski & Hoofnagle, *supra* note 87, at 323.

89. *Id.* at 327–30.

90. *Id.* at 337–40.

91. *Id.* at 342.

users and the license users obtain to use the work of others. Therefore, under the same contract, different terms, of course, merit a different analysis.

Moreover, the distinction between users and creators is not dichotomic. Users, and the public domain at large, as scholarship articulated, are not just recipients of the creative work, but also serve as generators of meaning, taking a meaningful part in the creative process.⁹² The digital revolution also transformed the creative process, which is now fueled by platforms and social networks.⁹³ Works are created in *communion*, in a consistent dialogue, while monetary incentives are playing a less prominent role in incentivizing user-generated content, as opposed to communicating and dialoguing with others.⁹⁴ Works of authorship are viewed as communicative acts and expressions of the author's autonomy as a speaking being,⁹⁵ while a copyrighted work serves as a speech addressed to the other, "an invitation to dialogue about ideas."⁹⁶ Under this communicative and dialogical view of authorship, users and the public domain are elevated from listeners, to de facto creators.⁹⁷ As such, limitations on the ability of users to access the work promulgated under contract not only affect secondary creation and the circulation of the original work, but the societal meaning attributed to the original work. While recognizing these limitations, employing this distinction is still useful for the purpose of judicial review of IP boilerplate terms, and the application of this distinction in the context of Unconscionability 2.0 is explored further in the following Parts.

92. See, e.g., CARYS J. CRAIG, COPYRIGHT, COMMUNICATION AND CULTURE: TOWARDS A RELATIONAL THEORY OF COPYRIGHT LAW 3 (2011); see also Lior Zemer, *Dialogical Transactions*, 95 OR. L. REV. 141 (2016) [hereinafter Zemer, *Dialogical Transactions*] (describing how authentic dialogue facilitates the creative process, and authorship operates as a dialogical act, as oppose to a communicative act).

93. See Perzanowski & Hoofnagle, *supra* note 87, at 323 (explaining the effects of the transition from physical to digital on music, media, and cultural consumption in the context of consumers' perceptions).

94. DRASSINOWER, *supra* note 48, at 55 (arguing that, as a matter of copyright law, "[A]n author is and must be an author among others. She speaks in a context that ensures conditions for dialogue"); see also Lior Zemer, *Copyright, Otherness, Dialogues*, 29 INTELL. PROP. J. 155 (2016) (providing a comprehensive review of this concept in Drassinower's theory); *infra* note 168 and accompanying text.

95. DRASSINOWER, *supra* note 48, at ch. 2.

96. *Id.* at 225.

97. Drassinower is a vital contributor to the communicative discipline in copyright. See Abraham Drassinower, *From Distribution to Dialogue: Remarks on the Concept of Balance in Copyright Law*, 34 J. CORP. L. 991 (2009); DRASSINOWER, *supra* note 48.

B. ADHERENT-USER IP BOILERPLATE

Society has shifted to the mass production of valuable digitized intangibles. IP is playing a more dominant role in the global economy and in promoting innovation than ever, a trend to be continued. Culture is created and disseminated on the Cloud and the Web, cultivated by technological platforms. As digitized mass production expands, so do form contracts that control the dissemination and commodification of valuable digital assets: regulating and assigning, and sometimes depriving one of, IP rights. When it comes to facilitating access to cultural assets, digitization can be a double-edged sword. On the one hand, it cultivates innovation and promotes dissemination by increasing access and reducing transactional costs,⁹⁸ and on the other hand, it subjects creative works to access limitations and restrictive terms, promulgated by form contracts and enforced by technological measures (Digital Rights Management Systems, or DRMs), a unique and powerful combination.⁹⁹ It is this shift into “cyberspace” that largely makes private ordering and contracts a dominant mode of IP regulation.¹⁰⁰

Scholarship has been exploring the interaction between form contracts and IP from the dawn of the Internet age. Many shared the observation that to a great extent, the promise of “creativity’s prosperity” in the information age has gone unfulfilled since corporations decided to use contract law (and, naturally, copyright law) as an axe to grind—and began appropriating intangible resources, expressions, and content.¹⁰¹ Some shared a “cautionary tale” about how copyright would die in 2010: a story in which all consumption of content is channeled and managed via one monopolistic technical system that requires users to click “I accept” on a strictly enforced form contract that displaced the legislative version of copyright law with a “pro-proprietor” version equipped

98. Scholars have viewed these benefits as suggesting that a contract-based “usage rights” model might be more efficient for consumers than copyright law. See Maureen A. O’Rourke, *Copyright Preemption After the ProCD Case: A Market-Based Approach Copyright Preemption*, 12 BERKELEY TECH. L.J. 53, 62, 70–71 (1997); Bell, *supra* note 41, at 561.

99. Bell, *supra* note 41, at 564. DRMs are technological protection measures used to control the access to, and restrict the use of, copyrighted materials to prevent infringing use. Sometimes they may also limit legitimate use.

100. Niva Elkin-Koren, *Copyrights in Cyberspace—Rights without Laws?*, 73 CHI.-KENT L. REV. 1155, 1156 (1998) [hereinafter Elkin-Koren, *Copyrights in Cyberspace*] (“Cyberspace facilitates such a regime by allowing information providers to distribute their works subject to contracts. The technical ability to make any access contingent upon accepting the terms of a license allows information providers to subject all users to standard terms of use.”).

101. See Niva Elkin-Koren, *Can Formalities Save the Public Domain? Reconsidering Formalities for the 2010s*, 28 BERKELEY TECH. L.J. 1537, 1537–38 (2013) [hereinafter Elkin-Koren, *Can Formalities Save the Public Domain?*] (“There is a wide consensus that copyright law has become a barrier for exploiting the full potential of the online environment in promoting creativity and creators.”).

with “innumerable accretions, modifications, and revisions” magnifying copyright owners’ rights.¹⁰²

Was this a detached dystopian tale or a vision of today’s digital reality? Instead of one system that controls access to content, consumption is managed on a small number of centralized platforms, using a slightly increased number of apps, but often under very similar sets of contractual terms, partially enforced by technology:¹⁰³ just as the authors envisioned.¹⁰⁴ Form contracts have only proliferated since this tale was first published and they continue to create different problems for different contingencies: creators, secondary creators, users of technology, consumers of cultural assets, and the public domain at large. Their impact transcends well beyond core IP policies, affecting public interests such as users’ privacy, information security, and free expression.

1. *Some Examples from Fair Use Waivers to the “Right-to-Repair” Your Smartphone*

Boilerplate has been displacing users’ rights for decades. As far back as 1999, when laying the theoretical foundations for ideas that ultimately developed into the “free culture” movement, Lessig observed that he might as well be barging through an open door, noting that “some will respond that I am late to the party: copyright law is already being displaced, if not by code then by the private law of contract.”¹⁰⁵ Two decades ago, Franklin and Reichman were also of the opinion that in virtual platforms, standard form

102. David Nimmer et al., *The Metamorphosis of Contract into Expand*, 87 CALIF. L. REV. 17, 20 (1999). Nimmer et al. proposed to revise U.C.C. Article 2B in light of the then-proposed Bill by Rep. Rick Boucher. According to this proposal, “non-negotiable” form contracts are unenforceable if they: 1) license or limit the use of uncopyrightable information; or 2) “abrogate or restrict” fair use limitations. *See id.* at 72–73. One opponent to this approach suggested that relying on the “non-negotiability” distinction is unsustainable and that this approach will undermine the (unprotectable) information economy. *See* Joel Rothstein Wolfson, *Contract and Copyright are Not at War: A Reply to the Metamorphosis of Contract into Expand*, 87 CALIF. L. REV. 79 (1999).

103. It is important to note though, that some IP boilerplate, mainly limitations on copying and modification by users, is not enforced at scale, unless enforcement is assisted by technological means such as Content ID and DRMs.

104. Nimmer et al., *supra* note 102, at 20–21.

105. LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 135 (1999) (suggesting that this was done mainly through the use of clickwrap contracts, shrinkwrap contracts, and end-user licenses, whereby “authors are increasingly demanding that purchasers, or licensees, waive rights that copyright law gave them.” Since these contracts are enforced merely by being “attached” and “knowable” in Lessig’s words, then already “through contract law, copyright holders can defeat the balance that copyright law intends”). Although almost two decades have passed, these insights continue to ring true.

contracts have virtually already superseded IP law.¹⁰⁶ In 2004, Radin claimed that “the widespread regulation of intellectual property rights by contract threatens, in principle, to undermine the official regime of intellectual property.”¹⁰⁷ Around that time, a substantial body of literature exploring how form contracts interact with copyright developed.¹⁰⁸

Prominent among this scholarship is Elkin-Koren,¹⁰⁹ who has dedicated a great deal of her scholarship to the problem of “private ordering” in IP. This scholarship articulates some key areas of concern. First, IP boilerplate (of the adherent-user type) often includes restrictive contract terms that prohibit the uses of information products that are generally allowed by copyright laws (such as fair use).¹¹⁰ The at-scale deployment of restrictive terms means that the usage of copyrighted work in a manner that is consistent with fair use,¹¹¹ for example,

106. J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PA. L. REV. 875, 878 (1999) (“In the networked environment . . . routine validation of mass-market access contracts and of non-negotiable constraints on users would tend to convert standard form licenses of digitized information goods into functional equivalents of privately legislated intellectual property rights.”).

107. Margaret Jane Radin, *Regime Change in Intellectual Property: Superseding the Law of the State with the “Law” of the Firm*, 1 U. OTTAWA L. & TECH. J. 173, 178 (2004) [hereinafter Radin, *Regime Change*].

108. See Cohen, *Lochner in Cyberspace*, *supra* note 76, at 538–59; Elkin-Koren, *Copyrights in Cyberspace*, *supra* note 100, at 1187–99.

109. See, e.g., Niva Elkin-Koren, *Copyrights in Cyberspace*, *supra* note 100, at 1200 (“[P]rivate ordering should not be immune from government regulation under freedom of contract doctrine because, as a general matter, such arrangements do not satisfy the doctrine’s underlying assumptions.”); cf. Niva Elkin-Koren, *What Contracts Cannot Do: The Limits of Private Ordering in Facilitating a Creative Commons*, 74 FORDHAM L. REV. 375, 420 (2005) (challenging the ability of Creative Commons licenses to genuinely promote access to creative work).

110. Elkin-Koren, *Contracting Copyrights*, *supra* note 2.

111. 17 U.S.C. § 107 (2018) (providing four non-exclusive factors for the courts to consider in determining whether a use of copyright protected-work is non-infringing. These include the purpose and character of the use, the nature of the copyrighted work, the amount of the copyrighted work used, and the effect on the market. For example, the dissemblance of code for the purpose of allowing interface and interoperability is considered fair use). See, e.g., *Sega Enter. Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1993); 17 U.S.C. § 117 (2018); see also PETER S. MENELL ET AL., *INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: 2018, VOL II: COPYRIGHTS, TRADEMARKS & STATE IP PROTECTIONS* 752–811 (2018) (providing a detailed overview of fair use).

for pure academic research purposes¹¹² or uses which are not “personal use,”¹¹³ is limited under mass-market contracts and licenses, although it is generally allowed under copyright laws.¹¹⁴ Such limitation on fair use affects the copyright system in its entirety and society more generally. It prevents access to the work by secondary creators and the public, thwarts commentary and criticism, and de facto rewrites the law to remove this vital limitation on ownership rights, and the “cultural bargain” the law represents.¹¹⁵ It also serves as a barrier to interoperability, innovation, and technical and scientific research, since restrictive terms often further limit the ability of the user to tinker with the work and perform actions such as decompiling, reverse engineering, and intermediate copying.¹¹⁶ It further undermines the democratic nature of

112. See, e.g., *Terms of Use*, FETLIFE (June 4, 2018), <https://fetlife.com/legalese/tou> [<https://perma.cc/8U2S-UM6V>] (stating under “Prohibited Conduct” that users might not “[u]se FetLife to do any academic or corporate research without the expressed written consent of BitLove [the owner]”). This, however, is a very unusual term. See *Sandvig v. Sessions*, No. 16-1368 (JDB), 2018 U.S. Dist. LEXIS 54339 (D.D.C. Mar. 30, 2018) (providing additional examples in the context of scraping).

113. See generally Bradley F. Abruzzi, *Copyright, Free Expression, and the Enforceability of Personal Use-Only and Other Use-Restrictive Online Terms of Use*, 26 SANTA CLARA HIGH TECH. L.J. 85 (2009).

114. See, e.g., 17 U.S.C. § 107 (1994) at the preamble; see also Kenneth D. Crews, *The Law of Fair Use and The Illusion of Fair-Use Guidelines*, 62 OHIO ST. L.J. 599, 607–37 (2001); THE COPYRIGHT OFFICE, SECTION 1201 RULEMAKING: SEVENTH TRIENNIAL PROCEEDING RECOMMENDATION OF THE ACTING REGISTER OF COPYRIGHTS 294 (Oct. 2018), https://www.copyright.gov/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf [<https://perma.cc/T7E2-4LLB>] (citing *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994)) (explaining in the context of security research that “many of the activities involved in security research are likely to be transformative, as the copying and alteration of the programs are for the purpose of providing information about those works—their susceptibility to security breaches—and do not ‘merely supersede the objects’ of the original creation”); *Authors Guild v. Google, Inc.*, 804 F.3d 202, 215–16 (2d Cir. 2015) (“[G]ood-faith security research promotes several of the activities identified in section 107 as examples of favored purposes, including criticism, comment, teaching, scholarship, and research.”).

115. See *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975).

116. See 17 U.S.C. §§ 117(a), 1201(f); THE COPYRIGHT OFFICE, *supra* note 114, at 168–72, 322–24 (discussing a variety of interpretability and jailbreaking activities under fair use analysis and noting that among others “interoperability is favored under the law”); see also *Sega Enter. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1514 (9th Cir. 1993); *Sony Computer Entm’t, Inc. v. Connectix Corp.*, 203 F.3d 596, 598–99 (9th Cir. 2000); Peter S. Menell, *Economic Analysis of Network Effects and Intellectual Property*, 34 BERKELEY TECH. L.J. 219, 244–52 (2019) (explaining that particular functional specifications, and processes and features “that affect access to or interoperability with a system” are excluded from copyright protection under 17 U.S.C. § 102(b) and the logic of *Baker v. Selden*, 101 U.S. 99 (1879), and that the Federal Circuit erred in *Oracle America, Inc. v. Google, Inc.*, 750 F.3d 1339 (Fed. Cir. 2014) in its analysis by subjecting the copying of functional specifications (in that case, Java APIs) to fair use analysis). In a later proceeding, the Federal Circuit further noted that verbatim copying for

societies built on the free exchange of information and ideas, and hinders free competition and innovation.¹¹⁷

Accordingly, scholarship explored the specific effects of contractual restrictions on reverse engineering and de-compiling and their effect on innovation, interoperability, and competition. Samuelson and Scotchmer noted that there is no “intrinsic reason” to allow contracts to circumvent “well-designed intellectual property regime[s],” “especially in markets with strong network effects.”¹¹⁸ Technologists warned, already in the early 2000s, that limiting the “the freedom to tinker,” and “the freedom to understand, discuss, repair, and modify technological devices that you own,” using restrictive contract language will hinder the positive externalities associated with tinkering.¹¹⁹ Commentaries recognized that the same vital concerns raised against the introduction of anti-circumvention regulation under the Digital Millennium Copyright Act (DMCA),¹²⁰ including restrictions limiting security

interoperability purposes is just a “moderately transformative activity.” See *Oracle America, Inc. v. Google, Inc.*, Tr. at 40:08–25 (2018) (Williams, Joint Creators II); see also Peter S. Menell, *Rise of the API Copyright Dead?: An Updated Epitaph for Copyright Protection of Network and Functional Features of Computer Software*, 31 HARV. J.L. & TECH. (SPECIAL ISSUE) 305 (2018).

117. See Menell, *Rise of the API Copyright Dead?*, *supra* note 116 at 318–22, 341–43; Menell, *Network Effects*, *supra* note 116 (explaining how section 102(b) limitations in appropriating functional elements needed for interpretability purposes serve the sound policy of promoting free competition and innovation); see also Motion of Consumers Union and Public Knowledge for Leave to File Brief of *Amici Curiae* in Support of Defendants-Appellants, at 1–9; *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005) (explaining how reverse engineering and interoperability foster market competition and sound public policy).

118. See Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1661 (2001). In Europe, since 1991, contract terms seeking to prevent decompilation have been considered void. See European Software Directive, *supra* note 178, art. 9(1), 1991 O.J. (L 122) at 45; see also Directive 2009/24/EC (analyzing the legal protection of computer programs and its implementation for example under German Copyright Act). Samuelson and Scotchmer further concluded that to “the extent that enforcement of anti-reverse-engineering clauses would have a detrimental effect on competitive development and innovation, legal decisionmakers may be justified in not enforcing them.” Samuelson & Scotchmer at 1630; see also Samuelson, *Freedom to Tinker*, *supra* note 58, at 582.

119. Mainly innovation, education and competition. See Whitfield Diffie, *11th USENIX Security Symposium San Francisco, California, USA August 5–9, Keynote Address, Information Security in The 21st Century*, 27(6); in LOGIN: THE MAGAZINE OF USENIX & SAGE 64, 66 (2002).

120. See, e.g., Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999).

testing,¹²¹ encryption research,¹²² and interoperability between systems, are relevant if contracts (instead of the DMCA) are used to enforce them at scale.¹²³

121. Recent empirical research conducted among security researchers shows that even though such restrictive terms are rarely enforced, they still create a chilling effect on research, causing “white-hat” security researchers, including researchers from academia, to adjust their research designs and methods, and in some occasions to avoid testing altogether. *See, e.g.*, CTR. FOR DEMOCRACY & TECH., TAKING THE PULSE OF HACKING: A RISK BASIS FOR SECURITY RESEARCH (2018) <https://cdt.org/insight/report-taking-the-pulse-of-hacking-a-risk-basis-for-security-research/> [<https://perma.cc/5HZJ-GRGZ>] (reviewing qualitative research conducted with twenty security researchers to explore their decision-making processes on whether to pursue security projects and activities, and finding that “[n]early half of the researchers interviewed mentioned the DMCA specifically as a source of legal risk . . . In some cases, researchers avoided working with devices and systems protected by access controls to eliminate the legal risks stemming from the DMCA”); *see generally* NAT’L TELECOMMS. & INFO. ADMIN. (NTIA), VULNERABILITY DISCLOSURE ATTITUDES AND ACTIONS: A RESEARCH REPORT FROM THE NTIA AWARENESS AND ADOPTION GROUP 2 (2015) (conducting a survey among 414 security researchers participating in coordinated disclosure, and finding that “[t]he threat of legal action was cited by sixty percent of researchers as a reason they might not work with a vendor to disclose”); *see also* Amit Elazari Bar On, *Private Ordering Shaping Cybersecurity Policy—The Case of Bug Bounties*, REWIRED: CYBERSECURITY GOVERNANCE (Ryan Ellis & Vivek Mohan Eds.) (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3161758 [<https://perma.cc/E2YJ-NB8R>]; *see also* Alexander Gamero-Garrido et al., *Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research*, 2017 PROC. 2017 ACM SIGSAC CONF. ON COMPUTER AND COMM. SECURITY 1501, 1503 (sampling seventy-five devices, sending the manufactures of these devices notices asking for permission to conduct security research on their products (one letter was from leading professors with tens of thousands of citations, one from an independent security researcher), evaluating their responses and finding that “most [of them] are loathe to surrender legal recourse and either are unwilling to engage on questions of permission or impose significant restrictions on doing so”). The authors also found “a significant difference in the responsiveness afforded to academic vs. independent security researchers.” *Id.* at 1502. Moreover, the authors surveyed more than 100 security researchers, and noted that twenty-two percent of them mentioned they were in fact threatened with legal action. *Id.* at 1511.

122. Samuelson, *Intellectual Property and the Digital Economy*, *supra* note 120, at 535–36; *see also* Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 BERKELEY TECH. L.J. 501 (2003). Since 1998, the DMCA already had a narrowly defined exception for encryption security research. *See* 17 U.S.C.A. 1201(j) (2018). Recognizing the limitations of this exemption, the Copyright Office introduced a temporary good-faith security research exemption in 2015, which was recently renewed and expanded. *See supra* note 20 (providing further discussion on the interaction between this specific exception and form contracts).

123. *See, e.g.*, Dan L. Burk, *Market Regulation and Innovation: Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537, 568 (2005) (noting that if use of mass-market licenses to prevent reverse engineering or interoperation of technically protected devices is “permissible, then boilerplate licenses might be employed to negate whatever limits have been placed on strategic overreaching by means of the DMCA anti-circumvention provisions”).

Other domains included the effects of contractual restrictions on various forms of fair use:¹²⁴ from parodying and criticism to academic research more generally.¹²⁵ For example, reviewing hundreds of terms, Moffat surveyed a variety of contractual restrictions, from limitations on modification of the work, limitations on commercial or “non-personal” use that might be covered under fair use,¹²⁶ and limitations on collection of non-protected material such as facts.¹²⁷

In specific domains like information security, scholarship focused on concerns related to the ability of software licenses to limit disclosure of software security evaluations,¹²⁸ a matter that recently was addressed in federal law with the introduction of the Consumer Review Fairness Act.¹²⁹

124. See, e.g., Moffat, *supra* note 43, at 45 (“Adhesion contracts, many of them now in clickwrap or browsewrap form, proliferate and govern nearly every commercial transaction and most of the ways in which the modern consumer interacts with the world. Virtually every one of these contracts contains a limitation on copyright’s fair use doctrine.”).

125. See, e.g., Gove N. Allen et al., *Academic Data Collection in Electronic Environments: Defining Acceptable Use of Internet Resources*, 2006 MIS Q. 599 (2006); see also Liu, *supra* note 122.

126. See Moffat, *supra* note 43, at 59.

127. *Id.* at 60; see Abruzzi, *supra* note 113, at 102.

128. See Jennifer A. Chandler, *Contracting Insecurity: Software License Terms that Undermine Information Security*, HARBORING DATA: INFORMATION SECURITY, LAW, AND CORPORATIONS 159 (ANDREA M. MATWYSHYN ed., 2009); see also Jennifer Stisa Granick, *The Price of Restricting Vulnerability Publications*, 9 INT’L J. COMM. L. & POL’Y 10 (2005).

129. Consumer Review Fairness Act, 15 U.S.C. §§ 45b(b)(1), (3)(E) (2018); see Chandler, *supra* note 128, at 176–77 (surveying, among others, reverse-engineering limitations and anti-benchmarking clauses in this context). Mulligan & Perzanowski suggest that in addition to the direct negative societal effects of decreased security, the case raised public attention to DRM technologies and corroded consumers’ trust in these systems, leading other vendors to reduce their investments in DRMs: a potential positive externality. See Deirdre K. Mulligan & Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L.J. 1157, 1166–77 (2007); *In re Sony BMG Music Entertainment*, FTC File No. C-4195 (F.T.C. June 29, 2007) <http://www.ftc.gov/os/caselist/0623019/0623019cmp070629.pdf> [<https://perma.cc/7TPL-Z>]32]. A similar effect occurred in the Cambridge Analytica data misuse case, in which the exploitation of data at large on the Facebook platform to manipulate election results, among others, by profiling, targeting, and influencing users led to a broader inquiry into the practices of social platforms and ad networks, and a consumer privacy global movement more generally. Still, this type of “consumer mistrust” externality could pose costs in areas like autonomous driving and medical connected devices, where there might be overall societal utility from using the device, yet one instance of a manufacturer’s alleged negligence causes consumers to doubt the system’s integrity, thereby undermining its adoption in the market. See Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 466–68 (2019) (providing a general discussion about the Cambridge Analytica scandal and its effects on data regulation).

Another body of literature was particularly concerned strictly with software and EULAs, and primarily with the proposed reform of U.C.C. Article 2B.¹³⁰ This bill was initially drafted as a proposed amendment to the U.C.C. and eventually became the Uniform Computer Information Transactions Act, 2000 model law (UCITA), which was not widely adopted.¹³¹ At the time, the American Law Institute and the National Conference of Commissioners on Uniform State Laws appointed a committee responsible for drafting a supplement to the U.C.C. § 2 in order to alleviate the uncertainty and confusion that gradually prevailed with respect to shrinkwrap licenses and their enforcement. To some extent, this reform compelled IP scholars to consider doctrinal solutions that are, in essence, contractual, inviting much-needed criticism of the contractual doctrines proposed under the bill.¹³² It also inspired scholars to deeply consider the implications of EULAs, specifically on IP policies. Reichman and Franklin noted that an “unbalanced approach” traditionally manifested in form contracts becomes even greater “when the adhesion contracts in question routinely implement the legal monopolies of intellectual property rights.”¹³³ As far back as 1999, they envisioned that this “deadly combination” between IP’s monopolistic rights and standard form contracts would become the primary vehicle to balance private property rights in intangibles with the public interest.¹³⁴

Thus far, we discussed how boilerplate interacts with fair use, but IP boilerplate also interacts with other doctrinal limitations on copyright ownership. Most prominently, the idea/expression and fact/expression dichotomies, which distinguish protectable expressive work from unprotected facts or ideas.¹³⁵ Copyright law excludes monopolistic protection in these

130. See Pamela Samuelson, *Intellectual Property and Contract Law for the Information Age: Foreword to a Symposium*, 87 CALIF. L. REV. 1 (1999); see also Nimmer et al., *The Metamorphosis of Contract into Expand*, *supra* note 102.

131. See UNIF. COMPUT. INFO. TRANSACTIONS ACT, 7 U.L.A. pt. II (2001) (adopted in Virginia and Maryland); UCITA, PRINCIPLES OF THE LAW OF SOFTWARE CONTRACTS, at p.1 (AM. LAW INST., Tentative Draft No. 2, 2005) (providing a later unsuccessful effort by the ALI to establish standards for software contracts).

132. See, e.g., Reichman & Franklin, *supra* note 106; see also Lemley, *Shrinkwrap Licenses*, *supra* note 23; Samuelson, *supra* note 128; Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089 (1998).

133. Reichman & Franklin, *supra* note 106, at 909.

134. The duo also criticized the drafters of the Article 2B bill for failing to recognize that standard form contracts operate more like property (rather than contractual) arrangements by virtue of creating “rights against all the world” through mass application. *Id.* at 910. The *ProCD* Seventh Circuit court, as I explore, followed the same erroneous path.

135. 17 U.S.C. § 102(b) (2018); *Baker v. Selden*, 101 U.S. 99 (1879) (holding that a while a textbook explaining a novel accounting system might be protected under copyright, that protection does not grant the copyright holder a monopoly over the use of the accounting

elements, which serve as building blocks for future creativity and innovation. But form contracts can be used to undermine these distinctions by allowing drafters to appropriate essential building blocks, excluding the public access to these elements, thereby creating de facto property monopolistic rights. This type of externality on the public domain interacts with fair use limitations, but extends beyond fair use limitations since it limits the ability of the user to use unprotected elements. In 1996, when the courts were faced with the question of enforceability of such restrictive terms in the matter of *ProCD*, considerable scholarly attention was given to this specific problematic interaction of IP boilerplate and copyright. Examples of these broader “public-domain” restrictive terms include limitations on scraping, copying, usage, modification, and collection of unprotected data mainly from websites and databases,¹³⁶ but also from journals and books, in library licensing contracts, for example.¹³⁷

More recently, a new type of IP boilerplate problem reignited scholarly debates around the limitations of the concept of ownership in the digital arena. The digital and connected era reconceptualized consumer consumption, affecting the understanding of traditional concepts of property and ownership.¹³⁸ Purchasing a physical book on Amazon gives the user a very different bundle of rights than purchasing the electronic “Kindle” ebook version. The electronic version comes with “strings attached,” all promulgated under the fine print language of the licensing contract.¹³⁹ The various limitations on the ability of users to enjoy the licensed copyrighted work are further enforced by technological measures. From a consumer standpoint, this type of IP boilerplate language raises unique questions since often, such limitations go far beyond what a reasonable user would expect, as empirical research shows.¹⁴⁰

This at-scale transition from physical consumption to digital consumption introduced pro-copyright owner boilerplate, DRMs, and Technological

system described in that book); *see also* *Lotus Dev. Corp. v. Borland Int'l, Inc.*, 831 F. Supp. 202 (D. Mass. 1993), 831 F. Supp. 223 (D. Mass. 1993), *rev'd*, 49 F.3d 807 (1st Cir. 1995), *aff'd*, 516 U.S. 233 (1996) (discussing the question of copyrightability of software menu command hierarchy); Menell, *Economic Analysis of Network Effects*, *supra* note 116, at 22–33 (discussing the copyright unprotectability of functional and network features).

136. *See supra* notes 111–117 and accompanying text.

137. *See, e.g.*, *Wright v. Warner Books, Inc.*, 953 F.2d 731, 741 (2d Cir. 1991); *infra* note 210 and accompanying text.

138. PERZANOWSKI & SCHULTZ, *supra* note 87.

139. *See* Perzanowski & Hoofnagle, *supra* note 87; Shaffer Van Houweling, *The New Servitudes*, *supra* note 80.

140. *See, e.g.*, Perzanowski & Hoofnagle *supra* note 87.

Protection Measures (TPMs) to all segments of cultural consumption.¹⁴¹ Even the consumption of tangibles and artifacts, like cars, mobile phones, and toaster ovens, became entangled with licenses and IP boilerplate language with the proliferation of connected devices. One specific type of boilerplate limitation in this domain sought to limit the right of the buyer of a connected product from repairing or inspecting the product or performing maintenance tasks on it. This type of limitation, which further gathered media attention, is deployed by John Deere, a leading tractor manufacturer that uses a combination of encrypted software and EULA language to “lock” consumers in and mandate that they repair and diagnose malfunctions in their tractors only in authorized dealerships that charge inflated fees. The language of John Deere’s license agreement explicitly prohibits reverse engineering of the software or transmission of the software over “any network or via a hacking device,” for any purpose.¹⁴² These types of restrictions affecting users’ right-to-repair are widely adopted in connected devices, from smartphones and voice assistants to medical devices.¹⁴³ Recognizing the societal costs of these limitations, the Copyright Office recently exempted the circumvention of software for the purpose of “diagnosis, maintenance, or repair” of a “smartphone or home appliance or home system.”¹⁴⁴

141. See, e.g., Deirdre K. Mulligan et al., *How DRM-based Content Delivery Systems Disrupt Expectations of Personal Use*, 2003 PROC. 3RD ACM WORKSHOP ON DIGITAL RTS. MGMT. 77; Deirdre K. Mulligan, *Digital Rights Management and Fair Use by Design*, 46 COMM. ACM 30 (2003); Julie E. Cohen, *Pervasively Distributed Copyright Enforcement*, 95 GEO. L.J. 1 (2006).

142. See *License Agreement for John Deere Embedded Software* § 4, JOHN DEERE https://www.deere.com/privacy_and_data/docs/agreement_pdfs/english/2016-10-28-Embedded-Software-EULA.pdf [https://perma.cc/9DUL-BVGZ]. This, notwithstanding the fact the Librarian of Congress exempted this circumvention from the DMCA under certain conditions already in 2015. See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 C.F.R. pt. 201 (2015). In 2018, this exception was broadened. See THE COPYRIGHT OFFICE, *supra* note 20.

143. Some states have advanced legislation to protect against these right-to-repair restrictions. See, e.g., Digital Right to Repair Act (providing an example of a specific law that supports consumers’ right-to-repair their cars in Massachusetts); Chaim Gartenberg, *California becomes the 18th state to introduce right to repair bill*, VERGE (Mar. 8, 2018) <https://www.theverge.com/2018/3/8/17097256/california-right-to-repair-bill-apple-microsoft-service-replace-parts> [https://perma.cc/BF7H-XQMD] (providing examples of right-to-repair bills that have been introduced in California and seventeen other states); see also Susan Talamantes Eggman, *Eggman Introduces Legislation to Create a “Right to Repair” for Electronics*, <https://a13.asmdc.org/press-releases/20180307-eggman-introduces-legislation-create-right-repair-electronics> [https://perma.cc/AUW8-Q6CP].

144. THE COPYRIGHT OFFICE, *supra* note 114, at 13; see *id.* at 3 (specifically addressing “the frustration of at the notion that copyright should prevent owners of devices from repairing, tinkering with, or otherwise exercising control over their own property” raised by the commentaries).

Still, contractual limitations extend beyond mere repairing to, more abstractly, limitations on the “right to tinker” with devices. Tinkering, as Samuelson explains, is a pillar of innovation and scientific progress.¹⁴⁵ Tinkering also helps one to establish relationships with property and the world more generally to define one’s identity and personhood.¹⁴⁶ In other cases, tinkering could save people’s lives.¹⁴⁷ But this type of tinkering is made more difficult as the “Internet of Bodies” culture expands and DRMs are deployed to limit patients’ access to their own medical information.¹⁴⁸ In the context of the freedom to tinker, form contracts are the main vessel to solidify what professor Ed Felten, a computer science professor, legal thinker, and “tinkerer,” called a “permission culture,”¹⁴⁹ in which tinkerers are punished for, threatened, or scared into avoiding tinkering, sometimes with no legal or

145. Samuelson, *Freedom to Tinker*, *supra* note 58, at 567; *see also* William W. Fisher III, *The Implications for Law of User Innovation*, 94 MINN. L. REV. 1417, 1455–72 (2010).

146. *See* Samuelson, *Freedom to Tinker*, *supra* note 58, at 565; Edward Felten, *The New Freedom to Tinker Movement*, FREEDOM TO TINKER (Mar. 21, 2013), <https://freedom-to-tinker.com/blog/felten/the-new-freedomto-tinker-movement/> [<https://perma.cc/K44Y-B3SR>]; *see also* Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957 (1982) (providing further discussion on the connection between property and IP and the counters of defining one’s self and personhood); Meir Dan-Cohen, *The Value of Ownership* (2000) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=189830 [<https://perma.cc/L2SU-E5DF>].

147. *See* Jason Koebler, *I’m Possibly Alive Because It Exists: Why Sleep Apnea Patients Rely on a CPAP Machine Hacker*, MOTHERBOARD VICE (Nov. 15, 2018), https://motherboard.vice.com/en_us/article/xwjd4w/im-possibly-alive-because-it-exists-why-sleep-apnea-patients-rely-on-a-cpap-machine-hacker [<https://perma.cc/6LPQ-JFVE>] (discussing a recent case in which a white-hat hacker from Australia spent approximately 1,000 hours circumventing “continuous positive airway pressure” medical device software DRM to allow the patients using it to access their medical information. The resulting open source tool, “SleepyHead,” enables patients to dramatically improve their medical situation). This type of conduct is now exempted from the DMCA but is still often barred under EULA language. *See supra* note 20. Perhaps such a limitation constitutes copyright misuse under the *WIREDATA* decision logic, since that patients’ sleep data is only available on the device, and it is their own data. *See* Assessment Techs. of WI, LLC v. WIREdata, Inc., 350 F.3d 640, 640 (7th Cir. 2003); *infra* note 208 and accompanying text.

148. Andrea M. Matwyshyn, *The ‘Internet of Bodies’ Is Here. Are Courts and Regulators Ready? A network of smart devices attached to or implanted in bodies raises a host of legal and policy questions*, WALL ST. J. (Nov. 25, 2018), <https://www.wsj.com/articles/the-internet-of-bodies-is-here-are-courts-and-regulators-ready-1542039566> [<https://perma.cc/U53J-ZWCK>].

149. *See* Felten, *The New Freedom to Tinker Movement*, *supra* note 146 (“Permission culture tells us that we don’t own the things we buy, that we are bound by contracts we have never seen, and that breaching those contracts is a felony punishable by years in prison.”). Here, Felten refers the potential interaction of the Computer Fraud and Abuse Act with the Terms of Use. *Id.*

societal justification.¹⁵⁰ If we are to create a “substantial zone of liberty” in which socially beneficial tinkering is allowed, as Samuelson suggested,¹⁵¹ then we must limit the exercise of mass-market contractual limitations and “technological boilerplate” in the IP realm.

2. *The Rise (and Fall?) of the “Patent-Wrap” Boilerplate: Limitations on the First-Sale Doctrine, Ownership, and the Sale/License Sham*

While IP boilerplate concerns are often discussed in the context of copyright, form contracts significantly affect patent law and the market for innovations. In fact, consumers and users interact with licensed patents hundreds of times per day, even in their home environment. Patents maintain our health and keep us entertained. Many of these patents are not acquired directly by the user from the patent owner (the patentee) or his manufacturer (the manufacturing-licensee), but purchased in secondary markets (for example, when a consumer is buying a used product). Limitations on secondary markets represent a notable area of interaction between contracts and IP, namely, contractual limitations on the first-sale doctrine and exhaustion.

The first-sale and exhaustion doctrines long served the elaborate task of balancing the monopoly power given to patent and copyright holders as proper incentive and the public interest in free markets.¹⁵² They are based on the “single-reward principle,” according to which the first authorized sale of the patented product exhausts the monopolistic power that is given to the patentee as a reward for her efforts and contribution to society’s advancement. Following the first sale, the patentee can no longer control the manner in which the patented product is sold or used in secondary markets, either by downstream purchasers or by sellers. Exhaustion and first-sale doctrines allow users to freely buy second-hand patented products (or products that contain patents), at a price that is not controlled by the patentee and is “restrictions-free.” The patentee can impose contractual resections on secondary markets, but she cannot use patent law for that purpose. This notion was reaffirmed by the Supreme Court decision in *Quanta*, which clearly stated that “the authorized sale of an article that substantially embodies a patent exhausts the patent holder’s rights and prevents the patent holder from invoking patent law

150. *Id.* (arguing that the permission culture is “punish[ing] [tinkerers] not for crossing boundaries or causing damage, but for acting ‘without authorization’”). The notion of “permission culture” is rooted in Lessig’s seminal work. LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, *supra* note 105.

151. Samuelson, *Freedom to Tinker*, *supra* note 58, at 565.

152. *See, e.g.*, *Bloomer v. McQuewan*, 55 U.S. 539 (1852) (providing an example of how the doctrine has been applied in case law since the nineteenth century). The doctrine is codified in copyright laws under 17 U.S.C. § 109(a) (2018).

to control post-sale use of the article.”¹⁵³

Still, the limiting doctrines of exhaustion and first-sale are often the subject of mass-market contractual abuse, as proprietors utilize form contracts, often enforced by technology, to reinstate the monopolistic power they cannot obtain under the IP regime, pushing the limits and boundaries of IP protection. One such type of abuse recently garnered the attention of the U.S. Supreme Court in the matter of *Lexmark*, perhaps the most influential patent exhaustion case in decades.¹⁵⁴ And in fact, the Court adopted a relatively broad conception of patent exhaustion, clarifying its roots in the common law principle of restraints on alienation, and the public policy considerations underlining it.¹⁵⁵ This “judge-oriented public policy” conceptualization of exhaustion, as Duffy noted,¹⁵⁶ might set the stage for invalidation of contractual terms based on public policy grounds, a view that at least one court already seems to have adopted, and aligns well with the proposed Unconscionability 2.0 solution.

The facts are straightforward. Lexmark sold, in the United States and abroad, its patented toner cartridges under two potential schemes: Consumers could buy the toner subject to an express “single-use” restriction, with a discount of twenty percent and a requirement to return to Lexmark when empty, or they could pay the full price and enjoy unrestricted use (and sale) of the cartridges. The manufacturer sells the printers at a relatively low price, charges a premium for the toner cartridges, and incorporates patents in the sold “refill” product, in this case cartridges, so it can use monopolistic power to control the market.

153. *Quanta Comput., Inc. v. LG Elecs., Inc.*, 553 U.S. 617, 637–38 (2008) (noting that it is well established that patentees can attach contractual restrictions to their products); *see also Keeler v. Standard Folding Bed Co.*, 157 U.S. 659, 666 (1895). The novelty under *Lexmark* was the ability to use patent law to enforce it (meaning, a claim for patent infringement). It is still, however, questionable if these contractual restrictions are enforceable in consumer settings. I explore this question in the following Sections.

154. *Impression Prods. v. Lexmark Int’l, Inc.*, 137 S. Ct. 1523 (2017).

155. *See id.* at 1532 (citing *Straus v. Victor Talking Machine Co.*, 243 U.S. 490, 501 (1917); *Keeler*, 157 U. S. at 667 (1895)) (explaining that such restrictive conditions have been “‘hateful to the law from Lord Coke’s day to ours’ and are ‘obnoxious to the public interest’” and that “[t]he inconvenience and annoyance to the public that an opposite conclusion would occasion are too obvious to require illustration”). The Supreme Court has also done so in the context of copyright first-sale doctrine. *See Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519 (2013).

156. John F. Duffy & Richard M. Hynes, *Common Law vs. Statutory Bases of Patent Exhaustion*, 103 VA. L. REV. ONLINE 1, 9 (2017) (“[I]f the [exhaustion] doctrine is based on an ‘affirmative policy’ of federal patent law favoring ‘the free movement of all patented goods’ . . . then the doctrine should not only be mandatory but might also render post-sale restrictions on use and resale unenforceable more generally, not merely unenforceable through infringement actions.”).

Impression Products acquired these “single-use” discounted cartridges, refilled the toners, and resold the cartridges in the United States without regard for the “single use” restriction or the authorization of Lexmark.

Lexmark brought suit against Impression (among others) for patent infringement under 35 U.S.C. § 271. Impression claimed, *inter alia*, that once Lexmark sold its cartridges to the consumers, the first buyers, it exhausted the patent rights in the cartridges. Simply put, the post-sale restrictions on reuse and resale of cartridges under Lexmark’s end-user agreements, could not be enforced as a matter of patent law.

The majority opinion in the *Lexmark* en banc decision at the Federal Circuit did not agree with Impression. It held that patent owners could impose restrictions on downstream use, resale of the patented products, and buyer’s post-purchase use—in other words, Lexmark could control the secondary market of the patent through unilaterally drafted restrictions.¹⁵⁷ The Federal Circuit allowed a patent owner to impose post-sale restrictions on downstream use and resale of a patented product: printer cartridges. These restrictions could be “communicated” through a standard form contract (package label), but enforced on third parties as a matter of patent law. For centuries, the application of the exhaustion doctrine balanced between the monopolistic right of the IP owner and public interest in market competition. Nevertheless, in *Lexmark*, the Federal Circuit allowed the rights’ owner to effectively “opt-out” from this fundamental doctrine by attaching a contract to the patented product. Simply put, patent laws established “historic” boundaries to the monopolistic right of the IP owner,¹⁵⁸ which could be redefined through a unilaterally drafted contract.¹⁵⁹

While U.S. patent law litigation frequently produces controversial decisions, it is not often that the prevalence of a centuries-old legal doctrine such as “exhaustion” is debated. As such, much ink (and printer toner) has been spilled on the Federal Circuit’s en banc decision in *Lexmark*. The case was granted certiorari following an animated public discussion (with over thirty amicus briefs) and numerous critiques, including from the government,¹⁶⁰

157. *Lexmark Int’l, Inc. v. Impression Prods.*, 816 F.3d 721 (Fed. Cir. 2016).

158. *Kirtsaeng v. John Wiley & Sons, Inc.*, 133 S. Ct. 1351, 1353 (2013) (referring to copyright first-sale doctrine).

159. See Molly Shaffer Van Houweling, *Exhaustion and the Limits of Remote-Control Property*, 93 DENV. L. REV. 951, 973 (2016) (“[T]he proper reach of the exhaustion doctrine is thus a question for IP policy—in Congress and the courts—not for IP owners unilaterally deciding that exhaustion should not apply to them, either by unilaterally placing post-sale conditions, re-characterizing sales as licenses, or imposing nominally contractual restrictions that are so adhesive and ubiquitous that they function like property rights.”)

160. The government filed a brief urging U.S. Supreme Court to review the case, and an additional amicus brief supporting reversal of the holding pertaining to contractual opt-outing

leading scholars,¹⁶¹ and retailers such as Costco.¹⁶²

The *Lexmark* case uniquely affected users as frequent consumers of patented products beyond the anticompetitive implications of imposing restrictions on secondary markets. This is because the main mechanism for imposing post-sale restrictions was not ordinary contracts, but rather standard form contracts. In other words, attention must be given not only to the question of what is an “authorized sale,”¹⁶³ but also what is the manner of authorization in which the restrictions are “communicated.” If the Supreme Court sustained the decision and allowed any patentee to impose contractual restrictions on the future use and resale of patents in every secondary market, by any user or reseller,¹⁶⁴ it would have provided patentees with incentives to draft longer form contracts with broader contractual restrictions for the sole purpose of invoking these restrictions in patent infringement cases against

from domestic exhaustion. See Brief for the United States as Amicus Curiae, *Impression Prods., Inc. v. Lexmark Int’l, Inc.*, 137 S. Ct. 546 (2016) (No. 15-1189), https://cdn.patentlyo.com/media/2017/01/15-1189_amicus_reversal_united_states.pdf [<https://perma.cc/W3K9-ZM5R>] (supporting reversal in part and vacatur in part).

161. Leading scholars have prepared and signed amicus briefs, written blogs, and published articles pertaining to the matter. See, e.g., Dennis Crouch, *Can Your Patent Block Repair and Resale and Prevent Arbitrage?*, PATENTLY-O (Jan. 31, 2017), <http://patentlyo.com/patent/2017/01/resale-prevent-arbitrage.html> [<https://perma.cc/P9WH-XEG8>] (summarizing a number of additional amicus briefs filed, and claiming that the Federal Circuit’s approach could undermine the market for the repair and reselling of goods); Brief of Amici Curiae Intellectual Property Professors and American Antitrust Institute in Support of Petitioner, *Impression Prods., Inc. v. Lexmark Int’l, Inc.*, 137 S. Ct. 546 (2016) (No. 15-1189) (explaining how the court in *Lexmark* strayed from 150 years of precedent by reframing exhaustion as a form of a default arrangement the patentees can simply contractedly opt-out from); PERZANOWSKI & SCHULTZ, *supra* note 87, at 155, 177–78 (discussing the manner in which contractual restrictions on the patent exhaustion doctrine have been historically treated in U.S. case law, analyzing *Lexmark* and critiquing it for radically rewriting the nature of consumer property interests in purchased chattels); see also Molly Shaffer Van Houweling, *Exhaustion and the Limits of Remote-Control Property*, *supra* note 159; Ariel Katz et al., *The Interactions of Exhaustion and the General Law: A Reply to Duffy and Hynes*, 102 VA. L. REV. ONLINE 8 (2016).

162. On Writ of Certiorari *Impression Prods. v. Lexmark Int’l, Inc.*, Brief of Costco Wholesale Corporation et al. as Amici Curiae in Support of the Petitioner, https://patentlyo.com/media/2017/01/15-1189_amicus_pet_costco_wholesale_corporation.pdf [<https://perma.cc/4BMG-N8ME>].

163. Naturally, much of the discussion remained focused on property theory, legal precedents concerning the exhaustion doctrine, and the proper interpretation of the language of 35 U.S.C. § 271(a) (2018).

164. See Petition for a Writ of Certiorari at 22, *Lexmark*, 137 S. Ct. 546 (2016) (noting that the Federal Circuit’s en banc decision in *Lexmark* “permits any patentee to foreclose the secondary market for any patented good . . . and enable[s] patentees to extract unjustified rents from downstream users”).

resellers.¹⁶⁵

The market's ability to police the quality of these contractual terms is limited due to the limited rationality of consumers, and consumers would be subjected to the informational burden associated with more disclosure, beyond the mere fact that private entities would now be allowed to use such contracts to re-write patent law's monopolistic limits.

C. ADHERENT-CREATOR IP BOILERPLATE

We create all the time. From reviews posted on Yelp to applications and innovative fashion designs submitted for the purpose of fulfilling academic commitments, to “forks” of software code posted on GitHub that are developed in commons, copyright-protected content¹⁶⁶ and innovations are created daily, by many, and they are regulated by form contracts in the absolute majority of cases.¹⁶⁷ In these cases, the boilerplate language is drafted by the nonowner of the content, and the adherent that accepts the terms is the original creator of the work. I have termed this contract the adherent-creator type of contract. This Part provides a brief overview of this type of contract. There is a vast literature encompassing the various types of such contracts and the implications of boilerplate in their context. Yet the literature neither addresses adherent-creator boilerplate as a category nor distinguishes it categorically from adherent-user boilerplate. The purpose of this Part is to shed light on some particular manifestations of adherent-creator boilerplate and explain why I claim they warrant this categorical distinction, which will further affect the application of Unconscionability 2.0 in their context. As such, this is not an exhaustive discussion of all types of these contracts.

1. *Social Networks and User-Generated Content: Cognitively Overburdened Creators*

As social media platforms proliferate and gain popularity, users continue to generate more content fueling these networks. This content, also known as user-generated content, ranges from selfies to mash-ups and mixes, and is created for a variety of motivations that often depart from the traditional monetary incentive-based utilitarian understanding of copyright.¹⁶⁸ Users often

165. Moreover, the case is the cornerstone of a number of landmark decisions of the Federal Circuit and the Supreme Court pertaining to the principle of exhaustion.

166. Much of the content being shared online satisfies copyright's low threshold to establish protection. These include the statutory requirements of originality and fixation set forth in 17 U.S.C. § 102(a) (2018) (“original works of authorship fixed in any tangible medium of expression”).

167. See Moffat, *supra* note 43, at 45.

168. See Elazari Bar On et al., *supra* note 82 (providing preliminary survey results of the author's research showing that from a sample of over 1,000 social media users, around sixty-

upload original content to express themselves and connect with others as a form of an extension of the self and its personality; they want to engage in communication and dialogue with others and take part in a social community; they want to share their “stories.”¹⁶⁹

But users not only create content with a click of a button—they also license and assign IP rights in their content with one click of a button, on the “clickwrap” or “browsewrap” ToS of the platform. Accordingly, scholarship has been raising some concerns addressing both the exploitation of user-generated content and users’ creativity by platforms, and the unreadability and complexity of these terms coupled with users’ bounded rationality.¹⁷⁰ A recent survey from 2017 found that 543 participants who joined a fictitious social network spent fifty-one seconds on average reading the ToU, with a ninety-three percent acceptance rate.¹⁷¹ In a survey conducted with the users later, researchers found that participants felt the policies are a “nuisance,” and ninety-eight percent of participants missed the intentional “gotcha clauses” the researchers implemented in the terms specifically mentioning users’ data will be shared for the purpose of assessing eligibility for “employment, financial service (bank loans, insurance, etc.), university entrance, international travel, the criminal justice system, etc.”¹⁷² and that users’ first-born child will be assigned to the platform as payment for accessing the network.¹⁷³

While users care about their rights in user-generated content, the information overload and complexity of ToS, as well as users’ dependence on social networks (that exhibit monopolistic features) leads them to waive their rights, regardless of their values and concerns. This could be characterized as the “user-generated content copyright paradox,” a phenomenon similar to the “digital privacy paradox” that persists in security and privacy—while users specifically report they deeply care about the privacy of their information, their actions—just minutes after reporting this—suggest otherwise.

five percent mentioned that they upload originally created content for “social interaction” purposes only).

169. See, e.g., Jordan Sundell, *Tempting the Sword of Damocles: Reimagining the Copyright/DMCA Framework in a UGC World*, 12 MINN. J.L. SCI. & TECH. 335, 337 (2011) (“[User-generated content] is creative content and published, usually by individuals who possess limited technical expertise, out of a desire to share, connect with others, or simply to express oneself.”). The popular social media network Instagram allows users to compile pictures and edit them into “stories.” See Instagram, *Stories | Instagram Help Center*, <https://help.instagram.com/1660923094227526> [https://perma.cc/2DPR-AP3S].

170. Elizabeth Townsend Gard & Bri Whetstone, *Copyright and Social Media: A Preliminary Case Study of Pinterest*, 31 MISS. C. L. REV. 249 (2012).

171. Obar & Oeldorf-Hirsch, *supra* note 32, at 1.

172. *Id.* at 7.

173. *Id.*

D. THE TECHNOLOGICAL BOILERPLATE: UNCONSCIONABILITY BY DESIGN

Private ordering in IP is not only accomplished through mass deployment of industry-wide boilerplate language. It is also facilitated, as scholarship has long observed,¹⁷⁴ by various modes of technology, architecture, and system design, that could give rise to potentially unconscionable technology. This prominent mode of regulation in IP operates in at least two prominent fashions: (i) technology that serves to enforce boilerplate language at scale, like the notable example of DRMs and TPMs enforcing IP rights holders' licenses, and (ii) technology that serves as boilerplate: enforcing rights and limiting statutory rights de facto, although there is no specific contractual arrangement in place. By virtue of this, technology could operate like in rem servitude-like property rights, since it operates against the world without any contractual relations in place.¹⁷⁵

A common example here is DRMs, TPMs, or other anti-circumvention technologies used in physical products, like CDs, printer cartridges, or other connected devices sold on secondary markets, where there is no direct contractual relation to the secondary buyer. And if technology is being used to enforce, limit, or deprive a statutory right beyond the contours of ToS, it moves from the first category to the second. Both categories undermine the statutory rights of users and creators, and when they are nonsalient and deployed at scale, may give rise to unconscionability by design.

Consider Content ID, a technology further discussed in Section III(B)(ii). In a nutshell, YouTube's Content ID system allows certain copyright owners to identify potential violations of copyright-protected content uploaded to the platform. Once content is uploaded, it is examined, and YouTube alerts the (alleged) owner about any (alleged) infringement and entrusts her with the full prerogative to determine the fate of the (allegedly) infringing content. Simultaneously, a Content ID claim is opened against the (alleged) offender, which consequently affects the ability of the "offender" to license his content

174. See LESSIG, *supra* note 105, at 20–21; see also Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance-by-Design*, 106 CALIF. L. REV. 697 (2018) (providing a comprehensive account of scholarship on governance by design from law, computer science, engineering, "socio-technical systems" and other disciplines, and surveying the rich literature in this field in a variety of contexts and case studies from privacy and cybersecurity to copyright and DRMs).

175. See, e.g., RADIN, *supra* note 1, at 46–51 (explaining how TPMs operate as boilerplate). For Radin, TPMs are the successors of boilerplate—they operate as the "machine rule" that replaces boilerplate. *Id.*

under a Creative Commons license or even to receive payments.¹⁷⁶

This system was characterized by Elkin-Koren as an example of a private mechanism for implementing “formalities,” meaning a procedural mechanism necessary for acquiring a valid copyright, such as registration, notice, and the like.¹⁷⁷ Formalities maintain a fine balance within the copyright regime—between the monopolistic rights of the current creator, and the remaining resources in the public domain that serve as building blocks for future creators. Content ID was heavily criticized by scholars as lacking transparency and due process.¹⁷⁸ It was also criticized for its lack of (technological) ability to distinguish between infringing content and content that is covered under copyright’s fair use doctrine.¹⁷⁹

YouTube’s ToS allows the streaming giant to decide if content is infringing copyright and remove such content without prior notice. YouTube also reserves the right to decide more generally if content violates the ToS “for reasons other than copyright infringement.”¹⁸⁰ But the ToS do not explicitly prohibit users from engaging in fair use activity, nor is it clear if such a term could be enforced.¹⁸¹ In fact, the ToS refer to YouTube’s policy guidelines,

176. See *How Content ID Works*, YOUTUBE (Sep. 28, 2010), <https://support.google.com/youtube/answer/2797370?hl=en> [<https://perma.cc/9LG5-PPCC>]; see also Taylor B. Bartholomew, *The Death of Fair Use in Cyberspace: Youtube and the Problem with Content ID*, 13 DUKE L. & TECH. REV. 66, 69 (2014).

177. See Elkin-Koren, *Can Formalities Save the Public Domain?*, *supra* note 101, at 1538, 1551.

178. See *id.* at 1560. Although YouTube revised the process to include a counter-notice, processed within the DMCA standard procedure, there is still room for change. See Diane Leenheer Zimmerman, *Copyright and Social Media: A Tale of Legislative Abdication*, 35 PACE L. REV. 260, 272 (2014); see also Matthew Sag, *Internet Safe Harbors and the Transformation of Copyright Law*, 93 NOTRE DAME L. REV. 499 (2017) (explaining how the DMCA notice-and-takedown regime, coupled with the emergence of automatic mechanisms such as Content ID and private agreements, render the importance of substantive copyright in the context of online expression).

179. *Takedown Hall of Shame*, ELEC. FRONTIER FOUND., <https://www EFF.org/takedowns> [<https://perma.cc/NC42-JX5H>].

180. *Terms of Service*, YOUTUBE §§ 6(G), 7(B) (May 25, 2018), <https://www.youtube.com/static?template=terms> [<https://perma.cc/4RSA-LN4C>].

181. It is questionable if that would have been possible, regardless of the tremendous reputational costs, in the aftermath of *Lenz*. In *Lenz*, YouTube removed a video uploaded by Stephanie Lenz, in which her toddler son was filmed dancing to the song “Let’s Go Crazy” by the artist Prince. The content was reported by Universal as infringing, although it is covered by the fair use protection under copyright law (17 U.S.C. § 107 (2018)). The trial court held that in light of the purpose of Article 17 U.S.C. § 512(f), Universal should have considered, in good faith, whether a particular use constitutes fair use prior to initiating the DMCA takedown process. Moreover, the court noted that such an “unnecessary removal of non-infringing material causes significant injury to the public.” *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150, 1155 (N.D. Cal. 2008). After lengthy litigation, Lenz indeed got compensated. In one of the later proceedings, the Ninth Circuit adopted a broad conception of fair use, explaining

which allow users to engage in authorized copyright activity.¹⁸² When YouTube’s Content ID takes down fair use-protected content beyond what is permissible under the ToS, its technology moves inside the second category to a design that displaces statutory rights, even though it does so without any contractual “anchor.” Of course, there are other examples, like TPMs used to prevent reverse engineering for the purposes of achieving interoperability, a fair use practice that is also exempted from the DMCA’s anti-circumvention provisions.¹⁸³ In this case, at least one proposed doctrinal solution should be looking at this *technology* as presumptively unconscionable, as if it was the boilerplate language itself. In Part IV, I discuss how Unconscionability 2.0 should be applied in this context.

E. A GAME OF CATCH? SOME EXISTING SOLUTIONS AND THE IP
BOILERPLATE PARADOX

This Article has already surveyed some of the existing IP solutions used to limit how private ordering using boilerplate language displaces or abuses IP policies, a question explored by many scholars.¹⁸⁴ These tools include specific rights that are inalienable, such as termination rights, as well as statutory limitations on certain IP rights assignments such as the new Consumer Review Fairness Act language barring assignment of consumer reviews’ copyrights¹⁸⁵ and state laws voiding assignment of employees’ inventions that exceed the scope of works-made-for-hire. But perhaps the most common way to protect IP from contractual abuse is judicial application of the overarching doctrines of preemption, misuse, and first-sale. Fair use is also sometimes used to that effect, but some courts have been willing to prioritize contracts, even standard form contracts, over IP law and enforce contractual restrictions on fair use.

The preemption doctrine,¹⁸⁶ which is discussed at length in the next Part, assures that the prerogative to further IP policy is vested in federal law, in order

that “[f]air use is not just excused by the law, it is wholly authorized by the law.” *See Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1151 (9th Cir. 2015). Yet in *Baystate*, a court in another Circuit discussed fair use as “statutory right” and still enforced a waiver of such right (to reverse engineer).

182. *Policies—YouTube*, YOUTUBE, <https://www.youtube.com/yt/about/policies/> [<https://perma.cc/P6JF-SJPK>] (“Only upload videos that you made or that you’re authorized to use.”).

183. *See* THE COPYRIGHT OFFICE, *supra* note 114; *see also* 17 U.S.C § 1201(f) (2018).

184. *See* Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827 (1998). A full account of these solutions is beyond the scope of this paper.

185. Still, one could claim this tool is in fact contractual in its essence, and is geared towards securing the rights of consumers and free competition, rather than traditional IP policies.

186. 17 U.S.C § 301(a) (2018).

to promote uniformity and prevent state laws from upsetting the fine balance dictated by Congress under federal law.¹⁸⁷ Preemption could have been the main way to address the tension between contract enforcement and IP policies at the federal level. Yet as I explain in the next Part, the opportunity was missed in the case of *ProCD*, and since then, as empirical research shows, courts have been unwilling to use preemption to void contracts.¹⁸⁸ First-sale and misuse, two other common law doctrines geared to prevent overexpansion of IP monopolistic rights that upsets the IP regime's fine balance, seem to have taken the front seat, both separately and combined, with the demise of preemption. The first-sale doctrine, (or exhaustion in patent law), played a dominant role in limiting post-sale boilerplate restrictions on how consumers use innovations and cultural artifacts.

Misuse, an affirmative defense to copyright or patent infringement, is aimed at preventing IP owners from exercising their monopolistic rights beyond or “outside” of IP’s legal scope. Such practice would be deemed a “misuse” of the owner’s right.¹⁸⁹ While misuse was originally focused on anti-competitive behavior, courts have recently expanded this traditional view to include essentially any violation of the public policy embodied in the grant of a copyright.¹⁹⁰

187. It draws its origins from the constitutional supremacy clause, U.S. CONST. art. VI, cl. 2. Subsection 301(a) provides that: “legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106 in works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright as specified by sections 102 and 103, whether created before or after that date and whether published or unpublished, are governed exclusively by this title. Thereafter, no person is entitled to any such right or equivalent right in any such work under the common law or statutes of any State.” The Copyright Bill of the 1979 act noted that “[t]he intention of § 301 is to preempt and abolish any rights under the common law or statutes of a State that are equivalent to copyright and that extend to works coming within the scope of the Federal copyright law.” See H.R. REP. NO. 94-1476 (1976), at 114; see also Lemley, *Beyond Preemption*, *supra* note 43; Niva Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*, 12 BERKELEY TECH. L.J. 93, 102 (1997) [hereinafter Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*] (providing an elaborate discussion). In the context of patents, the doctrine developed under case law. See *Sears, Roebuck & Co v. Stiffel Co.*, 376 U.S. 225 (1964); *Compro Corp. v. Day-Brite Lighting, Inc.*, 376 U.S. 234 (1964); *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141 (1989).

188. See Rub, *Copyright Survives*, *supra* note 36, at 1180 (reviewing 288 decisions of copyright preemption and finding that “[t]he Sixth Circuit is the only federal appellate court in the last twenty years to find a contract actually preempted by the Copyright Act”).

189. *Lasercomb Am., Inc. v. Reynolds*, 911 F.2d 970, 976 (4th Cir. 1990).

190. See *id.* at 978 (“The question is not whether the copyright is being used in a manner violative of antitrust law . . . but whether the copyright is being used in a manner violative of the public policy embodied in the grant of a copyright.”); see also *Alcatel USA, Inc. v. DGI Techs., Inc.*, 166 F.3d 772, 792 (5th Cir. 1999) (internal citations omitted) (holding that misuse is an “unclean hands defense” that “forbids the use of the [copyright] to secure an exclusive

In fact, almost a decade has passed since the Ninth Circuit noted that “the contours of [misuse] are still being defined,”¹⁹¹ and it still is very much the case. As such, courts have been using misuse to refuse to enforce (under copyright and patent law) a variety of contractual restrictions on IP rights.¹⁹² Misuse is thus becoming the de facto prominent vessel to keep boilerplate language in check. One recent case, *Disney v. Redbox*,¹⁹³ particularly illuminates this trend, discussing both misuse and first-sale while shedding light on some of the limitations of both these doctrines.

Disney sells combo packs with a DVD/Blu-ray disc version of its blockbuster movies alongside a download code that allows users digital access to the movie. Redbox operated a secondary market for Disney movies, renting DVDs and codes in kiosks, both separately and together in similar “combo packs.”¹⁹⁴ Disney sought to limit Redbox’s ability to sell the codes as a standalone product. Originally, Disney’s ToS, referred to in fine print at the bottom of the package and accessible online, prohibited the “sale, distribution, purchase, or transfer of Digital Copy codes”¹⁹⁵

Based on that language, in February 2018, the court found that Disney engaged in copyright misuse. Specifically, the court found misuse in the fact that Disney’s ToS required a user redeeming the code to represent that she is the current owner of the physical disc copy (when entering the code to download or stream the online version) as a condition to the online license. The terms therefore “purport[ed] to give Disney a power *specifically denied* to

right or limited monopoly not granted by the [Copyright] Office and which is contrary to public policy to grant”); *Assessment Techs. of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640, 647 (7th Cir. 2003); *Omega S.A. v. Costco Wholesale Corp.*, 776 F.3d 692, 699 (9th Cir. 2015) (“The defense of copyright misuse, however, is not limited to discouraging anti-competitive behavior.”).

191. *MDY Indus., LLC v. Blizzard Entm’t, Inc.*, 629 F.3d 928, 941 (9th Cir. 2010).

192. *Motion Picture Patents Co. v. Universal Film Mfg. Co.*, 243 U.S. 502 (1917) (refusing to enforce restrictions on the machines could be used beyond the point of the first sale); *Morton Salt Co. v. G.S. Suppiger*, 314 U.S. 488 (1942) (refusing to enforce a patent license requiring a patented article to be used only with another non-patented artifact produced by the patentee (salt tablets)); *Lasercomb Am., Inc. v. Reynolds*, 911 F.2d 970 (4th Cir. 1990) (refusing to enforce a software license provision limiting (in some manners) the use of the software and the development of a competing product, for ninety-nine years, beyond copyright’s protection period); *DSC Commc’ns Corp. v. DGI Techs., Inc.*, 81 F.3d 597, 601 (5th Cir. 1996) (refusing to enforce a copyright license requiring licensees to use only the copyright owner unprotected “microprocessor cards” on its phone switch operating system, thereby asserting protection over unprotected elements required for the development of interoperable cards).

193. *Disney Enters. v. Redbox Automated Retail, LLC*, No. CV 17-08655 DDP (AGRx), 2018 U.S. Dist. LEXIS 148489 (C.D. Cal. Aug. 29, 2018).

194. *Id.* at *2–3.

195. *Id.* at *4.

copyright holders by § 109(a) [codified copyright first-sale doctrine],”¹⁹⁶ causing users who want to enjoy the license to “forego their *statutorily-guaranteed right* to distribute their physical copies of that same movie as they see fit.”¹⁹⁷ This “improper leverage” of copyrights to restrict secondary transfers “directly implicates and conflicts with public policy enshrined in the Copyright Act” and therefore “constitutes copyright misuse.”¹⁹⁸

This broad conception of copyright misuse as essentially extending to any contractual language that places conditions on IP rights provided under the statute resembles to some extent the proposed model of presumptions of Unconscionability 2.0 discussed in Section IV(B)(i). One might claim that it takes this proposal even further, since the Disney court applied misuse in this manner where the “adherent” was a sophisticated commercial entity (Redbox) and not the typical adherent-user.¹⁹⁹

Disney changed their ToS to remove the above representation while still limiting the sale of the code separately and stating that only users who bought the code in a combo pack can redeem it, tying the code to the physical copy of the disc, but using different language. And so, in August 2018, the same court found that the misuse was “cured” (or there was no longer misuse), since “Combo Pack purchasers and recipients continue to enjoy digital access regardless whether they keep or dispose of the physical discs.”²⁰⁰ The court concluded that the “right to transfer a separate [c]ode” is not protected by the first-sale doctrine, and “[a] copyright misuse defense, therefore, is unlikely to succeed.”²⁰¹

This interesting distinction between physical copies and digital copies raises concerns since the sale of the code and the sale of the disc are essentially the same: in both cases, the user performs an action (inserting a disc into the DVD player or providing a code to a computer) to get access to the work. For users, this extra copy they bought via code was rendered useless, and for Disney the same result was achieved by limiting the secondary market of digital, and not physical, copies. Arguably, in today’s world where fewer people own a DVD player, the digital copy is much more valuable in secondary markets. Enforcing the first-sale doctrine in this manner does little to ensure that Disney’s monopoly does not extend beyond the law’s well-intended boundaries, especially in an era where the lines between sale and license, and

196. *Id.* at *18–19.

197. *Id.*

198. *Id.*

199. Similar to the Israeli court application of unconscionability in the matter of *Jobmaster*.

200. *Disney Enters. v. Redbox Automated Retail, LLC*, No. CV 17-08655 DDP (AGRx), 2018 U.S. Dist. LEXIS 148489 at *21–22 (C.D. Cal. Aug. 29, 2018).

201. *Id.* at 23.

physical and digital, are constantly blurred.²⁰²

Still, copyright misuse seems to be reconceptualized in *Disney* to extend to well beyond antitrust and anti-competitive effects to essentially a case that “upsets” the fine balance between owners and users under the law. In another case, *Omega S.A. v. Costco Wholesale Corp.*,²⁰³ the court explained that “[t]he limited scope of the copyright holder’s statutory monopoly . . . reflects a balance of competing claims upon the public interest: creative work is to be encouraged and rewarded, but private motivation must ultimately serve the cause of promoting broad public availability of literature, music, and the other arts,”²⁰⁴ and that the misuse at case was an “attempt to expand the scope of [the copyright owner’s] statutory monopoly” in a manner that upsets that balance.²⁰⁵

The recent application of the misuse and first-sale doctrines unveils an interesting narrative: U.S. IP regimes have been playing a game of catch with boilerplate. In certain cases, they seem to be particularly concerned with a specific displacement (for example, waivers of rights to reclaims of licenses or limitations on first-sale), in as much as they will specifically address the abusive practice via statutory limitations or specific case law. Then drafters of boilerplate quickly adapt: the record labels changed their boilerplate to categorize artists’ works as “made-for-hire” in the 1980s and 1990s,²⁰⁶ and Disney changed its ToS in 2018 to limit circulation of the access code and to bar the “separation” of combo packs. But drafters are not just changing contracts—they use technology to prevent users from engaging in legally permissible activities like fair use, copying, and access to unprotected data.²⁰⁷

202. See PERZANOWSKI & SCHULTZ, *supra* note 87; see also Robert A. Hillman & Maureen A. O’Rourke, *Principles of the Law of Software Contracts: Some Highlights*, 84 TUL. L. REV. 1519, 1523 (2009) (“[A]n end user’s right to ignore a term forbidding reverse engineering of the software should not depend on whether the parties labeled their transaction a sale or a license, but on the true substance of the deal and the term itself, including whether the term contradicts, for example, federal intellectual property law, state public policy or whether it is unconscionable.”); *Capitol Records, LLC v. ReDigi Inc.*, 910 F.3d 649, 659 (2d Cir. 2018) (finding that copyright first sale doctrine does not apply to digital files, but could be applicable to thumb drives with loaded digital files and that “other technology may exist or be developed that could lawfully effectuate a digital first sale”).

203. *Omega S.A. v. Costco Wholesale Corp.*, 776 F.3d 692, 699–700 (9th Cir. 2015), *cert. dismissed*, 136 S. Ct. 445 (2015).

204. *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975).

205. *Omega*, 776 F.3d at 705–06.

206. See David Nimmer & Peter S. Menell, *Sound Recordings, Works for Hire, and the Termination-of-Transfers Time Bomb*, 49 J. COPYRIGHT SOC’Y U.S.A. 387 (2001).

207. The latest 2018 DMCA exemption triennial proceedings provide a variety of examples of technological tools that do just that, and at scale: technological measures preventing educators and commentators from using short-clips of motion pictures, DRMs

And as drafters adapted, misuse (instead of preemption) became a more accessible tool to limit their abuse. While in *ProCD* the court allowed boilerplate language to exclude unprotected elements, such as phone records, from the public domain and prevent their copying, years later, in the misuse case *WIREDdata*,²⁰⁸ another court noted that limiting users' ability via contractual or technological means from accessing their own data, which is not protected under copyright, is "absurd" and may constitute copyright misuse.²⁰⁹ In another case involving contractual limitations on how authors use library materials such as manuscripts, the court interpreted the contract specifically in light of copyright policies, the subject matter of the contract at hand. The court noted that "to read the [contract] as absolutely forbidding any quotation, no matter how limited or appropriate, would severely inhibit proper, lawful scholarly use and place an arbitrary power in the hands of the copyright owner going far beyond the protection provided by law."²¹⁰ Finally, in *Disney*, a court in California expanded misuse to encompass terms that cause users to "forego their statutorily-guaranteed right," (in that case, the right of first-sale).²¹¹ While misuse is getting closer in function and scope to what preemption was perhaps meant to achieve, under some interpretations, it still has some notable limitations.

First, misuse is an affirmative defense that is only used by a user accused of patent or copyright infringement. As such, misuse is ill-equipped to address a core category I identified: the prominent case of the adherent-creator. Similar to first-sale and preemption doctrines, (even under the broader conception), misuse is focused on cases that involve abuse and unwarranted expansion of the monopolistic rights of the *owner* of the IP right. It therefore comes as no surprise that even in the most egregious of cases involving IP assignments, preemption or misuse were not invoked by the plaintiffs as a claim, but unconscionability was.²¹²

preventing reverse engineering and jail breaking, and more. *See* THE COPYRIGHT OFFICE, *supra* note 20.

208. *Assessment Techs. of WI, LLC v. WIREDdata, Inc.*, 350 F.3d 640, 647 (7th Cir. 2003).

209. *WIREDdata, Inc.*, 350 F.3d at 645 (holding that limiting access via other means (including technological) would be misuse: "We emphasize this point lest AT [Assessment Techs.] try to circumvent our decision by reconfiguring Market Drive in such a way that the municipalities would find it difficult or impossible to furnish the raw [unprotected, public domain] data to requesters such as WIREDdata in any format other than that prescribed by Market Drive [the proprietary software]. If [the owner] did that with that purpose it might be guilty of copyright misuse . . .").

210. *Wright v. Warner Books, Inc.*, 953 F.2d 731, 741 (2d Cir. 1991).

211. *Disney Enters. v. Redbox Automated Retail, LLC*, No. CV 17-08655 DDP (AGRx), 2018 U.S. Dist. LEXIS 69103 (C.D. Cal. Feb. 20, 2018).

212. *See I.C. ex rel. Solovsky v. Delta Galil USA*, 135 F. Supp. 3d 196 (S.D.N.Y. 2015); *infra* note 265; *see also* *Cubic Corp. v. Marty*, 185 Cal. App. 3d 438, 450 (Cal. App. 4th Dist.

Granted, these doctrines serve to secure the rights of secondary creators, but in the case of the original creator who is deprived of her rights, they offer little support. Second, because they are raised as a defense on a case-by-case basis, they still depend on litigation initiated by users, which rarely happens. Here, unconscionability and misuse share the same critique. Still, as explained in the following Part, unconscionability is somewhat limited by the narrow vision the United States has adopted for it, a vision that seems to be changing. Applying presumptions of unconscionability, creating affirmative rights, and encouraging (via fee-shifting) a consumer or a nonprofit advocacy group to petition for declaratory relief holding that a certain IP boilerplate term widely used in the industry is unconscionable, could have a broader impact: the application of the decision is not fact-dependent on the conduct and its purposes, or even on the specific adherent—only the boilerplate language.²¹³

Finally, the misuse and first-sale doctrines do not bar contractual enforcement of terms, just enforcement under IP laws.²¹⁴ But as some cases have shown, achieving the exact same perverse result using contracts, enforced at scale, could render IP limitations on monopolistic rights meaningless. Therefore, in some cases courts have been willing to stretch the application of misuse or first-sale to creatively weigh in on core matters of contract enforcement. In *Disney*, the court invoked such considerations in deciding whether a label on a box (a “box-top license”) stating “[c]odes are not for sale or transfer” and that “[the] product . . . cannot be resold or rented individually” could constitute an enforceable contract. Among other considerations,²¹⁵ the court noted that these statements provide the user with a “prescription [that] is demonstrably *false*, at least insofar as it pertains to the Blu-ray disc and DVD portions of the Combo Pack,” because “[t]he Copyright Act explicitly provides that the owner of a particular copy ‘is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy,’ ” and therefore “the *clearly unenforceable* ‘cannot be resold individually’ language conveys nothing so much as Disney’s preference about consumers’ future

1986); *Reach Music Publ’g, Inc. v. Warner/Chappell Music, Inc.*, No. 09 Civ. 5580(KBF), 2014 WL 5861984 (S.D.N.Y. Nov. 10, 2014); *Song Fi, Inc. v. Google Inc.*, No. 14-1283 (RMC), 2014 U.S. Dist. LEXIS 153436 (D.D.C. Oct. 29, 2014).

213. See Part IV.

214. See Section III(B)(iii) “A Limited Tool Set: From ProCD and Preemption to Lexmark and Exhaustion.”

215. Like the fact that Disney “ma[de] no suggestion that opening the box constitutes acceptance of any further license restrictions.” *Disney Enters.*, 2018 U.S. Dist. LEXIS 69103, at *11.

behavior, rather than the existence of a binding agreement.”²¹⁶ In *WIREData*,²¹⁷ the court noted that although the copyright owner did not sue for contract infringement, if it were to hypothetically “try by contract or otherwise to prevent the [defendants] from revealing their own data . . . [this] might constitute copyright misuse.”²¹⁸

Contrary to these opinions, the Supreme Court clarified that contractual limitations on the patent exhaustion doctrine are purely a question of contract law (and not patent law),²¹⁹ in line with decades-long precedent.²²⁰ The result is that even in the aftermath of *ProCD*, there is still an unclear picture as to what portions of IP law could be displaced by negotiated contracts or form contracts, under different doctrines, absent a clear provision in the law on inalienability.²²¹

I addressed *Lexmark* at length in Section II(B)(ii), and yet the apparent discrepancy in the application of first-sale doctrine in patents and copyright in the contractual context still raises questions. The *Lexmark* court clarified that both doctrines have their “roots in the common law principle against restraints on alienation,” and that “[d]ifferentiating between the patent exhaustion and copyright first-sale doctrines would also make little theoretical or practical sense” as the “two share a strong similarity . . . and identity of purpose.”²²² The statutory language of both doctrines is focused on the “authorization” of the owner.²²³ Does it matter that sources of “restraints” and limitations on

216. *Id.* at *12–13. (emphasis added).

217. *Assessment Techs. of WI, LLC v. WIREData, Inc.*, 350 F.3d 640, 647 (7th Cir. Wis. 2003).

218. *Id.* at 646–47.

219. *See* *Impression Prods. v. Lexmark Int’l, Inc.*, 137 S. Ct. at 1531 (“The single-use/no-resale restrictions in Lexmark’s contracts with customers may have been clear and enforceable under contract law, but they do not entitle Lexmark to retain patent rights in an item that it has elected to sell.”); *see also id.* at 1526 (“If the patentee negotiates a contract restricting the purchaser’s right to use or resell the item, it may be able to enforce that restriction as a matter of contract law, but may not do so through a patent infringement lawsuit.”).

220. *Bloomer v. McQuewan*, 55 U.S. 539 (1853).

221. *See* the discussion with respect to the “dispositive” nature of fair use under U.S. law in the aftermath of *Baystate* in Section III(B)(ii) “The Preemption Doctrine and the Contract-IP ‘Dichotomy.’”

222. *Lexmark*, 137 S. Ct. at 1527 (citing *Bauer & Cie v. O’Donnell*, 229 U. S. 1, 13, (1913)) (internal quotation marks omitted). The Court also clarified that “many everyday products are subject to both patent and copyright protections.” *Id.*

223. 35 U.S.C. § 271(a) (2018) and 17 U.S.C. § 109 (2018) (“[T]he owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.”); *see also Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519 (2013).

“authorization” originate from boilerplate contract or IP laws,²²⁴ where centuries ago, common law seemed to disfavor these restrictions even under negotiated contracts, as the Supreme Court observed in *Lexmark*.²²⁵ What will be the result if Lexmark actually decides to sue its consumers under contract law? The Supreme Court left open the question, which already had been left unanswered for centuries.²²⁶ Soon enough, courts will need to decide these questions again, and IP doctrines do not provide them with the tools to distinguish between negotiated and unnegotiated contracts. In fact, some recent misuse cases suggest that the lines between contract and IP laws are unintentionally becoming blurred, with some courts introducing IP policy into the discussion and some refusing to. I discuss this tension further in the following Part.

III. UNCONSCIONABILITY 1.0—A BRIEF HISTORY OF AN ALIENATING DISCOURSE BETWEEN CONTRACTS AND IP LAW

A. WHY UNCONSCIONABILITY?

The doctrine of unconscionability has been used for centuries to void contractual “unconscientious bargains.”²²⁷ In fact, some scholars trace the roots of unconscionability even prior to English law and Roman or Greek

224. See Shaffer Van Houweling, *The New Servitudes*, *supra* note 80.

225. *Lexmark*, 137 S. Ct. at 1532 (quoting Lord Coke in 1 E. Coke, *Institutes of the Laws of England* § 360, p. 223 (1628) and J. Gray, *Restraints on the Alienation of Property* § 27, p. 18 (2d ed. 1895)) (citing seventeenth-century sources, stating that “if an owner restricts the resale or use of an item after selling it, that restriction ‘is void, because . . . it is against Trade and Traffique, and bargaining and contracting between man and man [sic]’”) (“A condition or conditional limitation on alienation attached to a transfer of the entire interest in personalty [sic] is as void as if attached to a fee simple in land.”).

226. See *Quanta Comput., Inc. v. LG Elecs., Inc.*, 553 U.S. 617, 637, n.7 (2008) (“[The patent owner’s] complaint does not include a breach-of-contract claim, and we express no opinion on whether contract damages might be available even though exhaustion operates to eliminate patent damages.”); see also *Keeler v. Standard Folding Bed Co.*, 157 U.S. 659, 666, (1895) (“Whether a patentee may protect himself and his assignees by special contracts brought home to the purchasers is not a question before us, and upon which we express no opinion. It is, however, obvious that such a question would arise as a question of contract, and not as one under the inherent meaning and effect of the patent law.”).

227. See Hila Keren, *Guilt-Free Markets? Unconscionability, Conscience, and Emotions*, 16 B.Y.U. L. REV. 427 (2016); Colleen McCullough, *Comment: Unconscionability as a Coherent Legal Concept*, 164 U. PA. L. REV. 779, 787 (2016) (providing a comprehensive review of the origins of unconscionability).

traditions to the Torah and Jewish law, and notions of justice and reciprocity.²²⁸ As years passed, unconscionability became commonly used to mitigate the dangers that arise when one party to a contract enjoys supremacy of negotiating power and information—and the other is forced to “take it or leave it.”²²⁹ As Gibson mentioned, “[w]hen concerns about boilerplate arise, contract law turns to the unconscionability doctrine.”²³⁰

The origins of unconscionability in U.S. common law lay in England’s courts of equity,²³¹ and it was generally introduced in the United States in a Supreme Court decision from 1889.²³² It gained prominence in the United States in the late 1950s and early 1960s, following the adoption of the Uniform Commercial Code § 2-302 (U.C.C.) and the case of *Williams v. Walker*.²³³ Since then, it evolved into a fundamental part of U.S. contract law,²³⁴ an underlining principle,²³⁵ and “[o]ne of the most important developments in modern contract law.”²³⁶

228. Scott C. Pryor, *Revisiting Unconscionability: Reciprocity and Justice* (Sept. 14, 2018), <https://ssrn.com/abstract=3249449> [<https://perma.cc/EGK7-94YZ>].

229. *Id.* Yet, the application of Unconscionability is not limited to standard form contracts, nor to transactions that are governed under the U.C.C. See *Williams v. Walker-Thomas Furniture Co.*, 350 F.2d 445 (D.C. Cir. 1965).

230. Gibson, *supra* note 30, at 218.

231. It was later adopted in English common law, as well. See *Earl of Chesterfield v. Janssen*, (1751) 28 Eng. Rep. 82, 100 (defining an unconscionable term as one that “no man in his senses, not under delusion, would make, on the one hand, and which no fair and honest man would accept on the other”). This affirmation was later adopted by the U.S. Supreme Court. See *Hume v. United States*, 132 U.S. 406, 411 (1889).

232. *Hume*, 132 U.S. at 406. Although, in essence, it was also applied in a Tennessee state court case from 1834. *King v. Cohorn*, 14 Tenn. 74 (Tenn. 1834); see 1 WILLIAM FREDERICK ELLIOTT, COMMENTARIES ON THE LAW OF CONTRACTS 280 (1913).

233. *Thomas Furniture Co.*, 350 F.2d at 445.

234. See RESTATEMENT (SECOND) OF CONTRACTS § 208.

235. Keren, for example, uses the term “Unconscionability principle.” See Keren, *supra* note 227, at 432 (explaining that she uses “the term ‘principle’ rather than ‘doctrine’ to adopt Professor Eisenberg’s important argument that the unconscionability idea is broader than what arises from black-letter law and is a fundamental principle of modern contract law”).

236. Melvin Aron Eisenberg, *The Role of Fault in Contract Law: Unconscionability, Unexpected Circumstances, Interpretation, Mistake, and Nonperformance*, in *FAULT IN AMERICAN CONTRACT LAW* 82, 83 (Omri Ben-Shahar & Ariel Porat eds., 2010).

The unconscionability doctrine includes two components.²³⁷ The first component is procedural unconscionability, which pertains to inequality in bargaining power. Purportedly, when a standard form contract is offered on a “take it or leave it” basis, the contract is presumed to be procedurally unconscionable. Under the Restatement, a term that causes unfair surprise or that deprives the consumer of meaningful choice is procedurally unconscionable. This is determined by analyzing consumer awareness of terms in a market environment and establishing whether the term actually affects consumers’ contracting decisions.²³⁸ Simply put, if terms affect the decisions of enough consumers, they are salient, and the market disciplines their quality since drafters are incentivized to provide better terms—or consumers will choose the competition. Therefore, it would be harmful and redundant for courts to intervene via the unconscionability doctrine.²³⁹ Similarly, standard terms are not salient, even if they are properly disclosed and affirmed by signatures, clicks, or other methods, “because it is cognitively impossible to process and comprehend dense quantities of information packaged in standard forms.”²⁴⁰ In other words, the reporters of the Restatement clarify, courts have long been inquiring whether terms are salient under the procedural prong of unconscionability, without explicitly using the term:

The concept of salience underlies the metrics regularly used by courts to evaluate the procedural-unconscionability claim. For example, a “lack of meaningful choice” occurs when the terms do not affect consumers’ contracting decisions. Similarly, an “unfair surprise” occurs only when the terms were not salient. Other tests, such as “hidden” or “unduly complex” contract terms, or “uneven bargaining power” are either synonymous with, or direct results of,

237. According to the official comments to the U.C.C., case law has established a high threshold for both procedural and substantive unconscionability, requiring that the unconscionable term must amount to “oppression” or “unfair surprise” on the procedural level and “shocking the conscience” (in its one-sidedness) on the substantive level. *See, e.g.*, Lewis A. Kornhauser, *Unconscionability in Standard Forms*, 64 CALIF. L. REV. 1151, 1158, 1162 (1976); *Discover Bank v. Superior Court*, 36 Cal. 4th 148, 160 (2005); *see also* Arthur Allen Leff, *Unconscionability and the Code—The Emperor’s New Clause*, 115 U. PA. L. REV. 485 (1967)), (proposing that procedural unconscionability pertains to the contract formation process, while substantive unconscionability pertains to the content of the terms of the contract per se and their unreasonableness); *Industralease Automated & Sci. Equip. Corp. v. R.M.E. Enters., Inc.*, 58 A.D.2d 482 (App. Div. 1977). These are two cumulative conditions, judged according to a “sliding scale” approach. *See, e.g.*, *Armendariz v. Found. Health Psychcare Servs., Inc.*, 24 Cal. 4th 83 (2000) (quoting 15 WILLISTON ON CONTRACTS 226–27 (3rd ed. 1972)).

238. The Restatement, *supra* note 29, at 94.

239. *Id.* at 94–95.

240. *Id.* at 95.

nonsalience.²⁴¹

Moreover, the Restatement holds the view that most terms are nonsalient (meaning they do not affect consumers' decisions).²⁴² Indeed, after decades of mixed results, the Restatement finally leans towards adopting a view of unconscionability that moves beyond the issue of mere disclosure and procedure, clarifying that “[i]f courts were to focus on the criterion of salience, rather than on technical elements like disclosure, they would be able to avoid undesirable circumvention of the unconscionability test,”²⁴³ and that “[t]he salience criterion restores harmony between doctrine and policy.”²⁴⁴ Moreover, as the Restatement suggests, courts have been recognizing that form contracts are “procedural[ly] flaw[ed]” at their core. Their inherent flaw “is nothing more than the delivery of the terms in a nonnegotiable, standard-term document (sometimes labeled derogatorily ‘contract of adhesion’).”²⁴⁵ This has led courts to “set aside” the procedural prong of the test, emphasizing the substantive element instead under a sliding scale approach.²⁴⁶

This second component, substantive unconscionability, pertains to the question of whether the enforcement of the term would be “shocking to the conscience,”²⁴⁷ and addresses the one-sidedness of a term that unreasonably undermines “the consumer’s benefit from the bargain.”²⁴⁸

241. *Id.* (clarifying further that salience is also the test adopted by the U.C.C. and the test used to evaluate warranty disclaimers); see U.C.C. § 2-316(2), cmt. 1 (AM. LAW INST. & UNIF. LAW COMM’N) (defining the terms “conspicuous” and “unexpected and unbargained language of disclaimer”).

242. The Restatement, *supra* note 29, at 82; see also *id.* at 94 (“The great majority of standard terms are not salient, and such nonsalience alone—without additional procedural flaws—ought to meet the minimum quantum necessary for the procedural test. Accordingly, if standard terms are prima facie nonsalient, courts adjudicating an unconscionability claim can focus their attention on the substantive inquiry. And yet, if the standard form presentation of the term and its nonsalience are the only grounds for procedural unconscionability a greater quantum of substantive unconscionability would be required.”).

243. *Id.* at 95. The Restatement adopted the notion of salience in the Reporters’ notes and not the “black letter” or commentary parts.

244. *Id.* at 96.

245. *Id.* at 94.

246. *Id.*

247. *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593, 605 (E.D. Pa. 2007) (citing *Comb v. PayPal, Inc.*, 218 F. Supp. 2d 1165, 1172 (N.D. Cal. 2002)) (“A contract or clause is procedurally unconscionable if it is a contract of adhesion. A contract of adhesion, in turn, is a ‘standardized contract, which, imposed and drafted by the party of superior bargaining strength, relegates to the subscribing party only the opportunity to adhere to the contract or reject it.’”). However, as noted, courts have invoked a higher standard for procedural unconscionability, requiring “oppression” or an “unfair surprise.”

248. The Restatement, *supra* note 29, at 51.

Under the Restatement, since terms “are prima facie nonsalient, courts adjudicating an unconscionability claim can focus their attention on the substantive inquiry.”²⁴⁹ This focus on the substantive inquiry and the notion of salience “more closely tracks the doctrine’s normative underpinnings.”²⁵⁰ To summarize, the Restatement focuses on salience and the substantive inquiry, thereby bridging the gap between the Israeli and U.S. approaches, and laying the foundations to adopt Unconscionability 2.0.

Nevertheless, unconscionability has long been treated with hostility in U.S. law, by courts and scholars alike. This is but a part of the larger “ongoing debate regarding the desirability of utilizing this judicial power in a capitalist society.”²⁵¹ Scholarship warned courts about paternalism and judicial activism, and courts responded by rarely invoking the doctrine.²⁵² But this trend is shifting. Unconscionability is becoming more prominent and predictable. The Restatement reconceptualized the doctrine, and it is becoming a “coherent legal concept” that could be applied in a foreseeable manner, with lower thresholds.²⁵³ Unconscionability was given a “‘normative meaning’ which is consistent with the law and economics scholarship,” and a “‘jural meaning’ which is aligned with the reasonable expectations of consumers.”²⁵⁴

249. *Id.* at 94.

250. *Id.* A similar departure from the procedural inquiry under unconscionability may be noticed in a series of recent cases from California, where courts have emphasized the substantive inquiry instead of questions of consent and procedure. One district court noted that “whether a customer agreed to the terms had nothing to do with whether the terms were enforceable.” *Tompkins v. 23andMe, Inc.*, No. 5:13-CV-05682-LHK, 2014 U.S. Dist. LEXIS 88068, at *56–57 (N.D. Cal. June 25, 2014) (“23andMe [the drafter] contends that the arbitration provision cannot be procedurally unconscionable because the named Plaintiffs actually agreed to the TOS. . . . This conflates the requirements for contract formation with the question of unconscionability. . . . If 23andMe were correct that notice is ‘legally irrelevant’ to procedural unconscionability when the customer in fact agrees . . . then no disputed agreement could ever be procedurally unconscionable.”).

251. Keren, *supra* note 227, at 428; *see id.* at 432 (providing a useful summary of this debate in the context of unconscionability).

252. *Id.* at 444–49 (summarizing the “Anti-Conscience Approach” and the “free-market attacks” on the unconscionability doctrine following the *Williams v. Walker* decision in 1965). Keren focuses on two main arguments presented by law and economics jurists. First, courts should not intervene in market behaviors as long as both parties agreed to the contract, regardless of the exploitation of the offeree or notions of fairness or justice. Absent market failure, no legal intervention is required. Second, that consumers will be actually worse-off if contractual terms would be voided, since drafters will only draft sterner terms and raise the contract price. As Keren noted, behavioral law and economics literature exposed the market failures embedded in the bounded rationality of consumers, thereby supporting a more active use of unconscionability. *Id.*; *see also* Korobkin, *Bounded Rationality*, *supra* note 74.

253. McCullough, *supra* note 227, at 803–23.

254. *Id.* at 825.

Empirical research also shows that unconscionability is on the rise. Courts are receptive to the doctrine, finding more terms to be unconscionable, while expanding the various contexts in which the doctrine is analyzed.²⁵⁵ Litigants are gradually increasing their use of the doctrine.²⁵⁶ Landrum, who examined unconscionability case law in twenty states from 1980 to 2012, found that courts voided terms as unconscionable in twenty percent of the non-arbitration cases, and that there is now a more sophisticated understanding of unconscionability law.²⁵⁷ McCullough found that in the short period from 2012 to 2014, supreme courts in nine states invalidated terms as unconscionable.²⁵⁸ Knapp surveyed over 750 reported cases involving unconscionability in both state and federal courts from 1990 to 2008, and found a nearly tenfold increase in unconscionability claims, and growth in the relative rate of success of unconscionability claims.²⁵⁹

Unconscionability is no longer a “legal marginality”²⁶⁰ but has reemerged as a concept with a role to play both in the common law and statutory regulation.²⁶¹ It is the most appropriate doctrine for policing terms in adhesion contracts, as opposed to negotiated contracts that violate public policy in general.²⁶² The moral and equitable origins of unconscionability²⁶³ are familiar

255. These contexts obviously include arbitration and class-action waiver clauses, but are not limited to that. *See id.* at n.40; *see also id.* at 785 (providing analysis of the rise of unconscionability).

256. *Id.* at 787 (“From 2002 to 2012, state courts considered an average of 28.3 claims annually, compared to just 8.67 between 1980 and 2001.”).

257. Susan Landrum, *Much Ado About Nothing?: What the Numbers Tell Us About How State Courts Apply the Unconscionability Doctrine to Arbitration Agreements*, 97 MARQ. L. REV. 751, 779, 803 (2014).

258. For a total of twelve times. McCullough, *supra* note 227, at 786.

259. This is an increase from 16 in 1990 to 155 in 2008. *See* Charles L. Knapp, *Blowing the Whistle on Mandatory Arbitration: Unconscionability as a Signaling Device*, 46 SAN DIEGO L. REV. 609, 622–23 (2009).

260. Charles L. Knapp, *Unconscionability in American Contract Law: A Twenty-First Century Survey*, in COMMERCIAL CONTRACT LAW: TRANSATLANTIC PERSPECTIVES 309, 335 (Larry A. DiMatteo et al. eds., 2014).

261. *Id.* This role “both predates and transcends” the U.C.C., sale-of-goods law aspect of unconscionability. *See* Part IV.

262. This is usually governed under the Public Policy exception. *See* Farshad Ghodoosi, *The Concept of Public Policy in Law: Revisiting the Role of the Public Policy Doctrine in the Enforcement of Private Legal Arrangements*, 94 NEB. L. REV. 685 (2016).

263. *See* Keren, *supra* note 227, at 448–49 (explaining how, under the Pro-Conscience approach to unconscionability, the concept draws on judges’ moral sense or “moral conscience” and claiming that even the economic approach to unconscionability, inherently, rests its arguments on a moral basis).

to IP discourse.²⁶⁴ Unconscionability allows a more nuanced analysis of appropriating terms, one that considers information asymmetry and bounded rationality of users (salience), alongside IP considerations under the substantive prong. The latest *Lexmark* decision and the debate about using contracts with “informed” consumers, vis-à-vis licenses with sophisticated commercial entities in order to opt-out from patent exhaustion, illustrate why this nuanced analysis is useful.

Moreover, unconscionability is already invoked in IP contexts by litigators who ask courts to explicitly address IP policies when courts struggle to decide whether a term is unconscionable.²⁶⁵ Unconscionability is already being used in other jurisdictions, like Israel, to solve similar problems in IP contexts. Indeed, unconscionability is a standard, and as such it allows the flexibility required in order to analyze the variety and complexity of unexpected terms that drafters use in order to regulate new technologies. Yet, IP is a dynamic field. The majority of the problems that are caused by IP boilerplate require long-term regulatory solutions, but in the meantime, a standard will enable courts to provide a purposive answer that is based on the proper balance dictated by IP policies.

Unconscionability does not have to be an ambiguous “wild card.”²⁶⁶ Courts can tailor unconscionability to operate as a flexible standard with clear boundaries, and use it in a coherent manner similar to other standards used, such as patent and copyright misuse. The difference will be that Unconscionability 2.0 is rooted in both contractual and IP regimes, and reconciles the two.²⁶⁷ Unconscionability 2.0 could be accompanied by

264. See *infra* notes 494–496 and accompanying text (discussing the moral foundations of IP theory).

265. See *I.C. ex rel. Solovsky v. Delta Galil USA*, 135 F. Supp. 3d 196 (S.D.N.Y. 2015). In this case, a second-grade student participated in a competition conducted by a children clothing company, Miss Matched, in collaboration with her elementary school. Miss Matched later developed the student’s design to a full, successful line of clothing. The minor argued in her complaint that no contract was formed. The unconscionability claim was not pursued. Still, in a preliminary hearing the court struggled with the substantive unconscionability analysis. Solovsky claimed that term was unconscionable since “she was not provided compensation for sales of merchandise featuring the Hi/Bye design.” *Id.* (the court noted that Solovsky’s “simple drawing” creation “was prompted by the contest itself—rather than a design supporting an entire catalogue of merchandise” and therefore it is “has doubts as to whether plaintiff can demonstrate substantive unconscionability”). Clearly, the court could have benefited from an analysis which is more informed by IP policies.

266. RADIN, *supra* note 1, at 124 (claiming that “[t]he doctrine of unconscionability is a particularly salient kind of wild card”).

267. For example, the analysis does not ignore the critique of economics jurists who argue that courts should not interfere the market by voiding terms. It addresses them by explaining how nonsalient IP boilerplate creates market failures in this context. These failures are

mechanisms such as presumptions of unconscionability, and court preapproval of contracts, which will offer drafters more certainty. The time has come for U.S. law to reconsider its position regarding the feasibility of this doctrine in IP contexts. There is no reason to assume it will operate less effectively than the current “solutions.”²⁶⁸

B. THE UNDERUTILIZATION OF THE UNCONSCIONABILITY DOCTRINE IN IP SETTINGS

1. *The Chicken and the Egg: The Dismissal of Unconscionability in IP Scholarship*

The various problems created by IP boilerplate have not escaped the scrutiny of legal scholars, although the lion’s share of their attention has been directed at IP boilerplate in which the drafter of the contract is the IP owner, and in particular, to the EULA, an adherent-user type of boilerplate. Scholars noted that IP owners “who draft shrinkwrap license provisions often seek to expand their rights and limit the rights of users,”²⁶⁹ and that such expansions might undermine IP law’s purposes. As such, IP scholars devised a wide variety of solutions to the problem of appropriating contracts. Many relied heavily on regulation-based solutions, and firmly rejected any contractual solutions as insufficient.²⁷⁰ Others proposed various adaptations for ad hoc contractual tools that had been retrofitted to suit the virtual era.²⁷¹ Even though the issue does not apply to virtual realms alone, most of the literature was concerned with software and EULAs, and as mentioned, primarily with the proposed reform of U.C.C. Article 2B.²⁷²

externalities which the parties impose on society as a whole, when a user waives her right to perform a fair use in a copyrighted work or a patentee expands his monopolistic right.

268. See Rub, *supra* note 36 (providing discussion about the application of preemption as a “solution.” It should be noted that preemption also had its fair share of critiques); see, e.g., Radin, *Regime Change*, *supra* note 107, at 184 (claiming that “[p]re-emption is a very difficult and inconsistent area of doctrine”); Lemley, *Beyond Preemption*, *supra* note 43, at 113 (predicating that “preemption is unlikely to provide significant protection for the established rules of intellectual property law”). Lemley was right. See Rub, *supra* note 36.

269. See, e.g., Lemley, *Shrinkwrap Licenses*, *supra* note 23, at 1246.

270. IP scholars have suggested numerous legislative solutions, inviting legal reforms that regretfully have failed to come about. See Pallas Loren, *supra* note 46, at 535 (proposing that where a shrinkwrap or clickwrap agreement seeks to impose copyright limitations on ownership by restricting users’ rights, courts should presume that the relevant term constitutes copyright misuse).

271. Pallas Loren, *supra* note 46 (proposing a revised misuse doctrine).

272. See, e.g., Reichman & Franklin, *supra* note 106; see also Lemley, *Shrinkwrap Licenses*, *supra* note 23. The bill was initially drafted as a proposed amendment to the U.C.C. and eventually became the Uniform Computer Information Transactions Act, 2000 model law (UCITA): a model law that has been later abandoned. See *supra* notes 130–132.

Prominent among the early proponents of disciplining IP boilerplate, as mentioned, were Reichman and Franklin.²⁷³ They were also among the first to discard the general doctrine of unconscionability as inadequate. Unconscionability, they argued, rests too heavily on consumer perceptions, and therefore is of no use when seeking to achieve the elaborate balance required by IP law.²⁷⁴ At most, it could be used to address problems of information asymmetry between parties—and these are not the most critical issues created by such contracts.²⁷⁵

Other scholars shared their concerns, and many offhandedly announced the demise of unconscionability, dubbing it ineffective and inappropriate for accommodating IP policies. This is true regardless of the general focus of the policy solution-oriented discussion on the contractual arena.²⁷⁶ Lemley noted that “[c]ertain shrinkwrap license terms . . . may well be held unconscionable. But unconscionability is rarely used, and it is not well-tailored to the needs of intellectual property law.”²⁷⁷ Moffat asserted, in the specific context of fair use limiting doctrines, that although unconscionability (alongside the public policy limitation) could be “capable of addressing the issues raised by super-copyright provisions,”²⁷⁸ it is “poorly positioned to address questions of federal policy” as a primarily state-law tool, focused on procedural issues and assent, as opposed to federal copyright policy.²⁷⁹

Even the designated doctrine of unconscionability presented in the draft amendment to the U.C.C. Article 2B, and later codified under Section 105 of

273. Reichman & Franklin, *supra* note 106.

274. *Id.* at 927–28 (“Conversely, the unconscionability doctrine . . . is too consumer-driven to play the mediatory role between private and public interests that we envision. As formulated in Article 2 of the U.C.C., unconscionability directs judicial attention to surprising or oppressive terms in the context of specific transactions. . . . While proposed reforms of the unconscionability doctrine applicable to sales of goods merit careful attention, we doubt they would provide the kind of doctrinal tool needed to help courts preserve the dialogue between public and private interests in the digital environment that Article 2B is supposed to govern.”).

275. *Id.* at 928. The critical issues are the use of such contract to waive and re-draft IP regimes as formulated by courts and regulations: a use which undermines IP policies.

276. See, e.g., Lemley, *Beyond Preemption*, *supra* note 43, at 102–03 (noting that the “policy-driven debates [around copyright restrictive terms] have focused on issues surrounding contract law and theory” and that “the focus has been on contract law” while “[t]hose skeptical of “freedom of contract” above all’ also focus[ed] on contract law, relying primarily on state law doctrines to police the terms”); see also Cohen, *supra* note 94, at 475 (describing Professors Maureen O’Rourke and Tom Bell as viewing “contract as presumptively more efficient than copyright at promoting the dissemination of creative works”).

277. Lemley, *Beyond Preemption*, *supra* note 43, at 151.

278. Moffat, *supra* note 43, at n.257; see Nimmer, *Breaking Barriers*, *supra* note 184, at 873 (further noting that “[u]nconscionability as a theory lacks substantive or thematic focus”).

279. An assertion that could be challenged in light of the newly adopted Restatement. See *supra* note 29.

the UCITA,²⁸⁰ was not perceived as a suitable tool, as experience shows that the courts do not tend to void terms as unconscionable.²⁸¹ Samuelson and Opsahl observed that not only did case law rarely invoke the doctrine of unconscionability, but the standard imposed by the doctrine of unconscionability is too stringent, since it requires adhesive terms to not only be unreasonable, but also to be “shockingly oppressive.”²⁸²

This approach was reflected in later works as well, and many of the scholars who considered utilizing the doctrine as a possible solution for voiding IP boilerplate terms were also notably skeptical about the practical value of this proposition.²⁸³ Furthermore, the doctrine was presented as “useless” and meaningless in real-world business environments.²⁸⁴ Others

280. See *supra* note 272. Pursuant to subsection 105(b), the court may refuse to enforce a provision that is detrimental to fundamental public policies. (“If a term of a contract violates a fundamental public policy . . . the court may refuse to enforce the contract . . . to the extent that the interest in enforcement is clearly outweighed by a public policy against enforcement of the term.”)

281. See, e.g., Lemley, *Beyond Preemption*, *supra* note 43, at 163 (“[E]ven though Article 2B provides that substantively unconscionable contract terms will not be enforced, our experience with Article 2 cases makes it clear that courts rarely invoke the unconscionability doctrine to strike terms [and the] same will undoubtedly continue to be true in Article 2B cases.”). It should be noted that the drafters of the bill envisioned a narrowly defined doctrine, which critically differs from Unconscionability 2.0. In this respect, Nimmer commented that exceptions to enforcement should be allowed only in the event that “the competing public interest has sufficient strength and clarity to preclude the exercise of transactional choice by the parties.” Nimmer, *Breaking Barriers*, *supra* note 184, at 860; cf. Pamela Samuelson & Kurt Opsahl, *Licensing Information in the Global Information Market: Freedom of Contract Meets Public Policy*, 21 EUR. INTELL. PROP. L. 386 (1999) (providing an extensive discussion of the section’s legislative history). Elkin-Koren has notably dismissed the UCITA doctrine as too narrow and inadequate, as it was based on contractual solutions. See Elkin-Koren, *Contracting Copyrights*, *supra* note 2, at 211 (“The narrow limits on enforcement of contracts recognized by UCITA for protecting consumers and licensees are weak.”).

282. Samuelson & Opsahl, *supra* note 281, at 386.

283. See, e.g., Pallas Loren, *supra* note 46, at 510; see also David P. Sheldon, *Claiming Ownership, but Getting Owned: Contractual Limitations on Asserting Property Interests in Virtual Goods*, 54 UCLA L. REV. 751, 776–77 (2007) (“Virtual-world participants may also try to protect their interests in virtual items by attacking the terms of the EULAs under contract theories. . . . Existing case law tends to weigh against parties attacking EULAs on grounds of unconscionability.”); Bobby Glushko, *Tales of the Virtual City: Governing Property Disputes in Virtual Worlds*, 22 BERKELEY TECH. L.J. 507, 516 (2007).

284. Robert L. Oakley, *Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts*, 42 HOUS. L. REV. 1041, 1062 (2005) (“[P]otential is not realized, however, because in most cases the courts look only at the issue of unconscionability, which has a high threshold—much higher than ‘unfair’ or ‘indecent.’ Some have said that the threshold is either such a high bar or so vague or both that it is relatively useless in achieving a fair result.”). It is hard to blame the disheartened scholars, considering that even the U.C.C. Drafting Committee members noted that in ten years (from 1987 to 1997), U.S. courts found only fourteen clauses

expressed doubts that courts would find terms that are at odds with the purposes of IP policies, such as terms that prevent fair use, to be “shocking” enough to meet the high standard imposed by the doctrine of unconscionability.²⁸⁵

Elkin-Koren thoroughly analyzed unconscionability, along with other contractual doctrines, and reached the conclusion that “these doctrines are likely to offer only limited help in policing restrictive terms.”²⁸⁶ In her view, there are multiple grounds to support this conclusion. First, virtual realms are characterized by advanced distribution systems aimed to ensure that users shall have the required “opportunity to read.” Therefore, courts are unlikely to challenge disclosed terms.²⁸⁷ Second, since users fail to comprehend the extent of rights that copyright law affords them with respect to intellectual goods—in contrast, for example, to physical objects²⁸⁸—and are unable to predict the future use or revenue they will derive from them, users do not have sufficient incentive to read the terms.²⁸⁹ Third, since the use of “restrictive terms” is prevalent in contemporary practices, they fall under the definition of users’ “reasonable expectations,” and therefore courts will not regard such terms as an unfair surprise, bizarre, or oppressive.²⁹⁰ Fourth, it is difficult to meet the strict standards imposed by unconscionability, and to prove that an adhesive term is “so one-sided as to be unjust towards the user.” Therefore, if a user pays less for a product under a contract that includes a restrictive term, the transaction would be regarded as fair, despite the fact that this term negates values crucial to society as a whole.²⁹¹ Elkin-Koren further concludes that this contractual solution is to be discarded, as it concerns procedural terms that are irrelevant to the matter at hand. Contractual doctrines, in her view, lack the means that are required to solve the arduous problems created by restrictive terms in IP boilerplate. Therefore, we must abandon all hope of finding solutions in contractual disciplines, and look for answers beyond contract laws.

unconscionable under the doctrine. *See* U.C.C. § 2-105 cmt. 3 (AM. LAW INST. & UNIF. LAW COMM’N, Proposed Discussion Draft 1997), www.uniformlaws.org/shared/docs/ucc2and2a/ucc2am97.pdf [<https://perma.cc/WBA6-JHLJ>].

285. *See* Oakley, *supra* note 284, at 1064.

286. Elkin-Koren, *Contracting Copyrights*, *supra* note 2, at 200.

287. *Id.*

288. *Id.*

289. *Id.* (adding that therefore “contract rules that ask whether the user has had an opportunity to read the contract seem beside the point if users do not understand it”). This insight was raised by other scholars as well. *See, e.g.*, Moffat, *supra* note 43, at 56 (noting that “it would rarely be rational for consumers to bargain over super-copyright clauses”). Elkin-Koren uses the term “super-copyright” clauses to describe contractual terms that limit fair use terms. *Id.*

290. Elkin-Koren, *Contracting Copyrights*, *supra* note 2, at 200.

291. *Id.* at 202–03.

[C]ontract law in the United States seems ill-equipped to address the problem of restrictive terms It is concerned with protecting the expectations of the parties or aiding a party who is structurally disadvantaged in the bargaining process. It is not geared to protect public interest Classic contract doctrine recognizes no universal or social values beyond “freedom of contract” and the procedural safeguards are designed to secure it . . . contract doctrine does not provide a standard for distinguishing “good” terms from “bad” ones Consequently, one must look outside contract law for justifications permitting intervention in the allocation of risks fixed by the parties.²⁹²

Joining the commentators, recently Radin noted that because the application of unconscionability “is a process of relentless case-by-case adjudication, with many discretionary judgment calls” and “the outcomes are extremely unpredictable . . . [the doctrine] is not . . . well suited to evaluating and limiting large-scale boilerplate rights deletion schemes.”²⁹³ And so, despairing of the limited tools afforded by existing contract laws, some scholars abandoned the general doctrine of unconscionability, and moved to devise innovative doctrinal tools more suited to tackling the issue.²⁹⁴

Reichman and Franklin, for example, proposed a legislative solution—a revised “Doctrine of Public-Interest Unconscionability,” designated for transactions governed by the proposed U.C.C. Section 2B, to be codified in the framework of reform, which did not materialize.²⁹⁵ According to this proposed doctrine: “All mass-market contracts, non-negotiable access contracts, and contracts imposing non-negotiable restrictions on uses of computerized information goods must be made on fair and reasonable terms and conditions, with due regard for the public interest in education, science, research, technological innovation, freedom of speech, and the preservation of competition.”²⁹⁶

292. *Id.* at 204.

293. *See* RADIN, *supra* note 1, at 128–30 (noting that “[a]lthough thousands . . . of people may be subject to such a boilerplate scheme, only a few will bring suit challenging it . . .”).

294. *See* Reichman & Franklin, *supra* note 106, at 920 (“The common-law ‘public policy’ exception to the enforceability of contracts would, of course, logically apply to digital transactions, as would the doctrine of unconscionability codified in Article 2 of the U.C.C. In our view, however, these doctrines as currently administered give courts no solid foundation for coping with the downside social risks inherent in an unprecedented meshing of federal intellectual property policies with state-enforced contracts of adhesion.”). As an alternative, Reichman & Franklin have proposed a legislative solution—a revised “Doctrine of Public-Interest Unconscionability.” *Id.* at 930.

295. *See supra* note 131.

296. Reichman & Franklin, *supra* note 106, at 930.

A more general vision of unconscionability was imported from the U.C.C. and specifically adopted in the ALI Principles of Software Contracts,²⁹⁷ coupled with a very limited version of presumption of unconscionability, manifested by the Reporters' reference to the EU Directive on Unfair Contract Terms (93/13/EEC) as potentially informative for courts for purpose of the unconscionability analysis,²⁹⁸ and the inclusion of a list of suspected terms:

[T]erms that authorize the licensor to add spyware to the licensee's computer, that allow the licensor to modify the contract without notice or an opportunity to contest, that extend obligations automatically and without notice, that allow the licensor to change the nature of the software unilaterally, and that authorize cancellation without notice are suspect under [the] Principles.²⁹⁹

Yet this list is focused on contractual unfairness, procedure and formation, not pure IP matters.³⁰⁰ In fact, many of these practices are already unenforceable under general contract theory, have been found to be unconscionable by courts, and one of them (inclusion of spyware) is considered an unfair practice under the FTC Act.³⁰¹ By this virtue, this initiative missed a unique opportunity to provide courts with a more purposeful vision on how to apply the substantive prong of unconscionability in purely copyright-related clauses.

Several commentators dispute this view. They have refused to lose hope and envision the doctrine of unconscionability as a solution to the problem. However, even these scholars have persistently held certain reservations, and have presented unconscionability sporadically, with additional contractual tools to support the doctrine.³⁰²

297. Section 1.11 of the ALI, PRINCIPLES OF THE LAW: SOFTWARE CONTRACTS (2010). At comment 1, the reports state that Section 1.11 "reproduces § 2-302 of the U.C.C."

298. *Id.* at 1.11 cmt. c.

299. *Id.*

300. See Michael L. Rustad & Maria Vittoria Onufrio, *The Exportability of the Principles of Software: Lost in Translation?*, STETSON UNIVERSITY COLLEGE OF LAW RESEARCH PAPER NO. 2009-03, http://www.kentlaw.edu/faculty/rwarner/classes/internetlaw/2011/materials/rustad_onufrio_software_contracting.pdf [<https://perma.cc/U5ZB-WW5T>] (providing further discussion and a comparative analysis to the EU Directive list of restrictive terms (also focused on matters of procedure)).

301. See *In re Sony BMG Music Entertainment*, FTC File No. C-4195 (F.T.C. June 29, 2007); see also The Restatement, *supra* note 29, at 65, 79 (explaining the application of substantive unconscionability in the context of unfairness or deceptive practices and the doctrine of "Discretionary Obligations" that limits the enforceability of terms that "purports to grant the business absolute and unlimited discretion to determine its contractual rights and obligations" and are "unconstrained by the good faith obligation").

302. See, e.g., Cherenksy, *supra* note 31; Reichman & Franklin, *supra* note 106.

Hundreds of pages of scholarly literature have reviewed thousands of pages of U.S. case law, all leading to the ultimate conclusion that unconscionability is ill-equipped, ineffective, and contractually focused. But the lion's share of scholars' arguments for such dismissal originated in the narrow interpretation applied to the doctrine in U.S. case law. Discouraged by existing case law, scholars discarded this powerful doctrine as unhelpful, thus perpetuating the very same formalistic approach that dominated the doctrine in the first place, instead of rebutting it. Lacking the attention of such scholars, courts have been left with ineffective tools to face the problems at hand, issuing ill-advised rulings when required to address adhesive terms in IP boilerplate. This "chicken and egg" paradox accounts for one of the reasons as to why the doctrine of unconscionability was firmly rejected as a feasible solution in U.S. law.

While the dismissal of the doctrine might be understandable at the time, such arguments do not indicate that the doctrine is *prima facie* unsuitable. As suggested in the following Part, the sources of U.S. unconscionability were never grounded strictly in "an opportunity to read"; they never stipulated that only a "shocking" term merits voiding; and they were willing to acknowledge that a term of which an adherent is cognizant and to which she specifically agreed, and which comes as no surprise to her in any way whatsoever, shall be voided, provided that it is, in fact, unfair. They also acknowledged that the type of commerce that pertains to the contract shall determine the suitable and relevant expectations of the adherent. In the context of IP boilerplate, the relevant "type of commerce" concerns the policies of IP. The Restatement also facilitates such interpretations, focusing on the substantive inquiry that "applies to the contract as a whole."³⁰³

As some scholars admit, this doctrine could partially aid in cases of "extreme and unfamiliar contractual provisions" such as "no criticism" or "no parody";³⁰⁴ I claim further that it has a more substantial role to play in the IP realm, especially in light of the Restatement. As discussed in the next Section, contract law, and unconscionability in particular, allows for the application of extra-contractual considerations, including IP policies. Contract law certainly recognizes social values that go beyond "freedom of contract."³⁰⁵ It provides a standard by which one may "distinguish between 'good' and 'bad' terms."³⁰⁶ Contract law simply suffers from a formalistic interpretation that has led, prematurely as argued, to the abandonment of the powerful doctrine of unconscionability. In fact, a "[c]loser examination of the doctrine of

303. See The Restatement, *supra* note 29, at 63.

304. Rub, *Copyright Survives*, *supra* note 36, at 1217–18.

305. Paraphrasing Elkin-Koren, *Contracting Copyrights*, *supra* note 2, at 204.

306. *Id.*

unconscionability³⁰⁷ leads to the conclusion that it could be applied to IP boilerplate, and may even emerge as an effective solution.

2. *The Preemption Doctrine and the Contract-IP “Dichotomy”*

Thus far, the discussion focused on the underutilization of unconscionability in U.S. literature. This Section focuses on U.S. case law pertaining to IP boilerplate. Through a critical review of cases discussing both the *adherent-creator* and the *adherent-user* types of contract, I explain how an opportunity to utilize unconscionability from an IP perspective was missed, even when the contract in question pertained solely to IP rights. I further explain how the preemption doctrine contributed to this omission. To illustrate, I review *ProCD*, a landmark case that profoundly influenced the analysis of IP boilerplate in U.S. law.

In *ProCD*,³⁰⁸ which is notably recognized for addressing the question of enforceability of shrinkwrap contracts, the United States Court of Appeals for the Seventh Circuit avoided a material discussion on drafters’ abilities to rewrite IP laws and appropriate the public domain. It also established the “No-Preemption” approach to contracts, one that would dominate U.S. laws for the following years.³⁰⁹

As explained, according to the preemption doctrine,³¹⁰ the prerogative to regulate copyright is vested in federal law in order to induce uniformity and prevent state laws from upsetting the fine balance dictated by federal law.³¹¹ In *ProCD*, the plaintiff invested millions of dollars in the creation of a telephone book that contained more than 95,000,000 records.³¹² Had this book been printed, it would have required tens of thousands of pages; therefore, the plaintiff chose to market it as a CD. The CD was accompanied by a standard form contract of the shrinkwrap type. This contract included various provisions that prohibited users from harvesting the records in the CD, copying them, or making them accessible to other users on the Internet or on

307. Paraphrasing Pallas Loren, *supra* note 46, at 509.

308. *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

309. *See* Rub, *Copyright Survives*, *supra* note 36.

310. 17 U.S.C. § 301(a) (2018).

311. *Id.* (“[L]egal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106 in works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright as specified by sections 102 and 103, whether created before or after that date and whether published or unpublished, are governed exclusively by this title. Thereafter, no person is entitled to any such right or equivalent right in any such work under the common law or statutes of any State.”); *see also* Niva Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*, *supra* note 187, at 102.

312. *ProCD, Inc. v. Zeidenberg*, 908 F. Supp. 640, 644 (W.D. Wis. 1996).

any “other networked or time-shared environment.”³¹³ The defendant, Zeidenberg, purchased a copy of the CD and in March 1995 began producing a virtual phone database using the records of ProCD and records derived from an additional company’s directory. This newly created online database was later integrated with software created by Zeidenberg,³¹⁴ which allowed Internet users direct access to the records for a more competitive price compared with that offered by ProCD. The problem began when the ProCD database was found to be excluded from the protection of copyright law in the post-*Feist* era.³¹⁵

The trial court sought to prevent drafters from rewriting IP laws under contracts, monopolizing what the law left to the public domain. It found that the purpose of the restrictions under the EULA, limiting the harvesting of data, was in fact “an attempt to avoid the confines of copyright law and of *Feist*.”³¹⁶ It further concluded that as copyright policies, and more particularly the *Feist* ruling, actually enable the plaintiff to create the database by harvesting information from 3,000 other databases, it is inconceivable that the plaintiff should thereafter deny others a similar right.³¹⁷ In other words, if you used building blocks that are in the public domain for your own creation, you cannot deny others the right to act likewise. Just as copyright law allowed you access to the public domain, you cannot use contract law to deny that access to others. The court therefore emphasized that “the rules of the game have not changed,”³¹⁸ and clarified that U.S. federal copyright law preempts the

313. *Id.* at 645 (“You will not make the Software or the Listings in whole or in part available to any other user in any networked or time-shared environment, or transfer the Listings in whole or in part to any computer other than the computer used to access the Listings.”).

314. The only component of the CD that was effectively protected under copyright law was the proprietary software created by ProCD; however, this software was not copied by the defendant in a commercial manner, but only in a manner protected under 17 U.S.C § 117. *See id.* at 648–50. Ostensibly, Zeidenberg copied exactly what he was allowed to copy under the *Feist* ruling: phone records which, according to *Feist*, are not protected under copyright laws. *Feist Publ’ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991). Likewise, ProCD also acted exactly to the degree *Feist* allowed it, in harvesting the data from 3,000 other telephone books. *See ProCD, Inc.*, 908 F. Supp. at 659–60; *see also* DAVID MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 3.04 (2015).

315. *See ProCD, Inc.*, 908 F. Supp. at 647.

316. *Id.* at 657, 659 (concluding that “[this] prohibition on the distribution of public information cannot be squared with the purposes of copyright law or with plaintiff’s own compilation of data”); *see also id.* at 658 (“Contracts that seek to protect reproduction and distribution rights step into territory already covered by copyright law. It would alter the ‘delicate balance’ of copyright law to allow parties to avoid copyright law by contracting around it.”).

317. *Id.* at 659.

318. *Id.*

provisions of this IP boilerplate.

This outcome is, of course, desirable. However, to a certain extent, it is such use of the preemption doctrine in early case law that contributed to the underutilization of unconscionability in IP. It allowed the courts to use the hammer (preemption) in order to avoid the enforcement of the contract, instead of the chisel (unconscionability). By leaving the question of enforcement to contract law, a division was created between IP law (on the federal level) and contract and consumer law (on the state level). And so, as the division between the two deepened, a dichotomy emerged. In other words, if copyright law preempts state legislation, when a matter pertaining to federal copyright law is concerned and the contemplated contractual provision pertains to copyright, such as restrictions on fair use,³¹⁹ then state contract law doctrines are deemed no longer necessary. Presumably, this solves the problem; difficulties that are created by adhesive provisions that seek to disrupt and negate the purposes of IP policies are solved by the most appropriate tools of all—IP law doctrines.

Alas, the preemption doctrine was interpreted in this respect as a double-edged sword.³²⁰ If the contractual provision was not preempted by federal law, then the question of enforceability is left solely to contract laws, where little, if any, attention is given to promoting the purposes of IP policies.³²¹ This argument is further illustrated by the discussion of the Seventh Circuit in *ProCD*:

319. See Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*, *supra* note 187, at 101.

320. See NIMMER & NIMMER, *supra* note 314, at n.97 and accompanying text (criticizing such narrow usage of section 301, proposing instead to examine, in a broader sense, whether or not the contract at hand seeks to undermine copyright law).

321. See, e.g., Lemley, *Beyond Preemption*, *supra* note 43, at 151. Some scholars argue that there is also an inter-contractual dichotomy pertaining to the question of contract enforceability, whereby the courts are willing to reach binary results, concluding that the contract is either formed—and is therefore enforceable—or was not formed, and therefore is unenforceable. On the other hand, courts are unwilling to analyze the fairness of the transaction or whether the consideration, in the relevant circumstances, is adequate. See KIM, *supra* note 23, at 192 (“Under current law, contractual assent is an ‘all-or-nothing’ proposition—either a contract is formed in its entirety or it is not. A finding of contract formation means that the non-drafting party has the burden of raising a contract defense, such as unconscionability, to escape enforcement. But as previously noted, courts are generally reluctant to evaluate the fairness of a bargain or the adequacy of consideration. The battle then is often lost at the formation stage—a properly formed contract will be enforced unless the terms are so egregious that it outweighs judicial reluctance to evaluate terms.”); see also James Gibson, *Boilerplate’s False Dichotomy*, 106 GEO. L.J. 249 (2017) (explaining how “courts and commentators alike view boilerplate as necessary to the modern transaction. When asked to set boilerplate aside, then, they confront a dichotomy: either enforce boilerplate terms or wreak havoc on the consumer economy.” Gibson claims this dichotomy is false).

Must buyers of computer software obey the terms of shrinkwrap licenses? The district court held not, for two reasons: first, they are not contracts because the licenses are inside the box rather than printed on the outside [Contract law] second, federal law forbids enforcement even if the licenses are contracts [Preemption Doctrine] . . . we disagree with the district judge’s conclusion on each. Shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general (for example, if they violate a rule of positive law, or if they are unconscionable) [Contract laws]. Because no one argues that the terms of the license at issue here are troublesome [from a contract law perspective], we remand with instructions to enter judgment for the plaintiff.³²²

The Seventh Circuit in *ProCD* changed the rules of the game on two levels. First, it ruled that a shrinkwrap contract is in fact contractually valid, and second, it laid down the prevalent interpretation of the preemption doctrine, an erroneous interpretation later adopted in *Baystate*. Rights that are created by a contract, the court argued, affect no one but the parties thereto, and they prevent nothing on the part of the general public, which is why they are not exclusive rights in terms of the preemption doctrine.³²³

The majority opinion in *Baystate* followed the same path.³²⁴ The heart of the legal dispute was a shrinkwrap contract that prohibited reverse engineering. *Baystate* argued that its right to reverse engineer the product is covered by the

322. *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1448–49 (7th Cir. 1996); see also *ProCD, Inc.*, 908 F. Supp. at 650 (differentiating between questions pertaining to the enforcement of the contract on the grounds of the adherent’s lack of bargaining power, and questions arising from the fact that the contract at hand seeks to replace federal copyright law with private ordering. The court held: “In addition to raising issues of enforceability, shrinkwrap licenses also pose important questions about the extent to which individual contract provisions can supplement or expand federal copyright protection. It is important to analyze these licenses carefully, not only to determine their validity but also to ascertain whether they are preempted by the Copyright Act”).

323. *ProCD, Inc.*, 86 F.3d at 1454 (“A copyright is a right against the world. Contracts, by contrast, generally affect only their parties; strangers may do as they please, so contracts do not create ‘exclusive rights.’”). But see Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*, *supra* note 187, at 102–04 (claiming that private ordering produces rights with outcomes similar to rights in rem and that “the introduction of new distribution technologies blurs the distinction between rights in personam and rights in rem”); NIMMER & NIMMER, *supra* note 314, at § 1.01, § 19D.3 (explaining that generally, there are two conditions for applying the doctrine. The first requires that the right pertains to copyright “subject matter,” meaning an intangible asset such as a work of art that is protected under copyright laws, but also including intellectual resources that remain in the public domain, such as ideas. The other requires that the claim concern rights that are equivalent to the exclusive rights of copyright).

324. *Bowers v. Baystate Techs.*, 320 F.3d 1317 (Fed. Cir. 2003).

fair use protection under copyright law,³²⁵ and therefore the restricting contract should be preempted. This argument was rejected by the court, which based its ruling, *inter alia*, on *ProCD*. The court ruled that a license that denies fair use is, by its nature, a contract, and such a contract cannot create “exclusive rights” as required by the preemption doctrine.³²⁶

Among other cases cited by the court was the decision in *Canal Electric*,³²⁷ where the court agreed to recognize a contractual modification of a statutory right only when the purpose of the right is “protection of the property rights of individual parties . . . rather than . . . the protection of the general public”³²⁸ and only when the waiver does not harm the purposes of the relevant legislative enactment.³²⁹ It is this reference from which the court in *Baystate* derived its conclusion that “case law indicates the First Circuit would find that private parties are free to contractually forego the limited ability to reverse engineer a software product under the exemptions of the Copyright Act.”³³⁰

It follows that in the majority’s opinion, not only does a shrinkwrap contract constitute a properly executed contract, and users’ waivers of fair use are considered knowing and voluntary, but likewise, the fair use protection regulates the rights of individuals and has nothing to do with the general public.³³¹ The court in *Davidson* sided with the majority opinion in *Baystate*,³³² and its decision further demonstrates the dichotomy created by the current use of the preemption doctrine in case law concerning IP boilerplate.

The district court sided with the majority opinion in *Baystate*. The defendants, it was argued, waived their right to fair use when they entered into

325. 17 U.S.C. § 107 (2018); *see, e.g.*, *Atari Games Corp. v. Nintendo of Am., Inc.*, 975 F.2d 832, 1015 (Fed. Cir. 1992); *Bateman v. Mnemonics, Inc.*, 79 F.3d 1532, 1539 (11th Cir. 1996); *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1527–28 (9th Cir. 1992).

326. *Baystate*, 320 F.3d, at 1325.

327. *Canal Elec. Co. v. Westinghouse Elec. Corp.*, 548 N.E.2d 182 (Mass. 1990).

328. *Id.* at 378.

329. *Id.* (“A statutory right may not be disclaimed if the waiver could ‘do violence to the public policy underlying the legislative enactment.’”).

330. *Baystate*, 320 F.3d at 1325–26.

331. *Cf.* Motion of Consumers Union and Public Knowledge for Leave to File Brief of Amici Curiae in Support of Defendants-Appellants, *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005) (explaining, in detail, how restrictions on reverse engineering and fair use are harmful to public policy and competition, and displace core IP policies). In addition, the majority opinion did not consider at all the fact that this waiver was done via a standard form contract, while the minority opinion emphasized the adhesive nature of the contract, and noted that a situation whereby the standard form contract preempts copyright law and restricts fair use is both absurd and unjust. *Baystate*, 320 F.3d at 1337.

332. *Davidson & Assocs. v. Internet Gateway*, 334 F. Supp. 2d 1164 (E.D. Mo. 2004) *aff’d*, 422 F.3d 630 (8th Cir. 2005).

the agreement, and the court must enforce the waiver.³³³ The court further ruled that the preemption doctrine does not apply, specifically because the parties created, through the contract, another right that is not an existing right in copyright law, i.e., “the right to restrict the use of the software through the EULAs and TOU,” and therefore created an “extra element”³³⁴ that distinguished between the contractual right and the exclusive right. A reasonable consumer, the defendants argued, would not pay \$50.00 for a game that he cannot use.³³⁵ And so it comes as no surprise that the court, having based its entire reasoning for the non-applicability of the preemption doctrine on the fact that the parties created in the license other rights that do not pertain to the purposes of copyright, avoided addressing the purposes of IP policies in its narrow analysis of unconscionability.³³⁶

333. *Id.* at 1181 (“The Court finds the reasoning in *Bowers* persuasive. The defendants in this case waived their ‘fair use’ right to reverse engineer by agreeing to the licensing agreement. Parties may waive their statutory rights under law in a contract. . . . In this case, defendants gave up their fair use rights and must be bound by that waiver.”).

334. *Id.* at 1175 (quoting *Nat’l Car Rental Sys. v. Comput. Assocs. Int’l*, 991 F.2d 426, 433 (8th Cir. Minn. 1993)) (“The Court agrees that the contractual restriction does create a right not existing under copyright law. The right created is the right to restrict the use of the software through the EULAs and TOU. ‘Absent the parties’ agreement, this restriction would not exist. The contractual restriction on use of the programs constitutes an extra element that makes this cause of action qualitatively different from one for copyright.’ Therefore, the Court finds that the EULA and TOU are not statutorily preempted by the Copyright Act If an extra element is required, instead of or in addition to the acts of reproduction, performance, distribution or display, in order to constitute a state-created cause of action, then the right does not lie ‘within the general scope of copyright’ and there is no preemption.”).

335. *Id.* at 1179.

336. The *Davidson* district court found that the contract is not procedurally unconscionable, since the defendants had a choice whether to purchase another game, or to decline the license and return the game to the store. In addition, the defendants are sophisticated consumers; they are software programmers who understand the legal language included in the contract. Finally, the terms and conditions of the contract lack a surprise element: the defendants knew that using the game would be subject to their consent to the end-user license, and had thirty days in which to review the agreement and return the game. The court determined that the contract is not substantively unconscionable, as the terms and conditions of the license, which restrict the users’ right to fair use, “do not impose harsh or oppressive terms.” *Id.* at 1180; *cf.* *Motion of Consumers Union and Public Knowledge for Leave to File Brief of Amici Curiae in Support of Defendants-Appellants* at 21, *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005) (explaining why such a provision should be deemed unconscionable, since, among others, the “Blizzard EULA and TOU demand the waiver of important and well-established rights that benefit the public” and “enforcement of the reverse engineering and matchmaking clauses would preclude . . . innovative and competitive behavior . . . [and] interoperable competitive services . . . [a] result [that] would profoundly affect the marketplace for software products and services and disrupt the public policy objectives underlying intellectual property law”).

The Eight Circuit, reviewing the case *de novo*, agreed.³³⁷ The court cited *Baystate*,³³⁸ and found that “[p]rivate parties are free to contractually forego the limited ability to reverse engineer a software product under the exemptions of the Copyright Act[,]” and so can “a state permit parties to contract away a fair use defense or to agree not to engage in uses of copyrighted material that are permitted by the copyright law if the contract is *freely negotiated*.”³³⁹ Signing a EULA, the court clarified, falls under “freely negotiating” a contract.³⁴⁰ Here the court cited the dissent from *Baystate*, but failed to recognize its critical point: the distinction between “freely negotiated contracts” from contracts of adhesion, which are “no different in substance from a hypothetical black dot [state] law” and that can “extensively undermine the protections of the Copyright Act.”³⁴¹

This is, therefore, the dichotomy at its worst, characterized by two stages. First, the court must determine that the contemplated rights are not IP by nature, or do not affect third parties so that it can overcome preemption, and find the contract as a whole enforceable. Second, the court is required to address unconscionability and the question of enforcement in terms of contract law, and it therefore refrains from turning to the purposes of IP law (on the federal level). The answer is therefore left to contract and consumer law (on the state level). Given this dichotomy, the purposes of IP law yield to the contractual doctrine, and the narrow approach to unconscionability in case law prevails. D’Agostino characterized this phenomenon more broadly as the general principle of freedom of contract, or contract law *lex rex* as hindering copyright’s *lex specialis*.³⁴²

The following example reviews a adherent-creator type of contract, where unconscionability was still underutilized: a contract that seeks to regulate the IP rights of the non-drafter, and is perhaps one of the world’s most influential IP boilerplate, impacting the copyrights of billions of users. Unconscionability is still underutilized because the adherent in this case is not an “ordinary” consumer—he does not pay (money) for the product. He uses the platform “free” service, paying with his IP rights.

337. *Davidson & Assocs. v. Jung*, 422 F.3d 630 (8th Cir. 2005).

338. *Bowers v. Baystate Techs., Inc.*, 320 F.3d 1317, 1325–26 (Fed. Cir. 2003).

339. *Davidson*, 422 F.3d at 639 (emphasis added).

340. *Id.* (“By signing the TOUs and EULAs, Appellants expressly relinquished their rights to reverse engineer.”).

341. *Baystate*, 320 F.3d at 1337 (Dyk, J., dissenting).

342. *Cf.* D’Agostino, *supra* note 47, at 4–5 (explaining further that this could result in “copyright law objectives [are] undermined as authors go unrewarded and unprotected, left to their own devices to engage in protracted litigation with symbolic results”).

In *Song Fi*,³⁴³ a number of plaintiffs, including Song Fi, an artist named Brotherton, and Brotherton's six-year-old son, sued YouTube for unlawfully removing the video "Luv Ya" from its platform. Song Fi, a small Washington, D.C. corporation holding distribution rights of independent creators, uploaded to the YouTube sharing platform a video in which a band of artists named Rasta Rock Opera, as well as Brotherton and his son, all appear. After two months, YouTube removed the video, arguing that the video violated its terms of use, since the user allegedly committed various manipulations of the video's view-counting system through electronic means. Song Fi argued that this was untrue, and appealed YouTube's decision to remove the video, but YouTube refused to put the video back online.³⁴⁴

Confident in their position, Song Fi, alongside other plaintiffs, sued YouTube for defamation, breach of contract, and other claims. One of the plaintiffs' arguments was that the YouTube's ToS was, in general, an unconscionable contract.³⁴⁵ In regards to procedural unconscionability, the court inquired as to whether the plaintiffs lacked significant ability to choose the terms of the contract.³⁴⁶ The plaintiffs argued that given the market power of YouTube as a video-sharing platform, and the fact that Song Fi is a small, independent corporation in the music business, they had no choice but to accept the terms and conditions of YouTube's contract.

The court rejected this argument completely. It found that the fact that the platform is popular does not demonstrate a lack of choice by its users—they can, for example, upload the video on an independent website.³⁴⁷ The court also rejected the substantive unconscionability argument. The plaintiffs argued that the contract includes several adhesive provisions, including the provision whereby YouTube can completely (and immediately) remove any user content at YouTube's own exclusive discretion.³⁴⁸ This is the same provision through which YouTube legitimizes, at least on a contractual level, *ex ante*, the

343. *Song Fi, Inc. v. Google Inc.*, No. 14-1283 (RMC), 2014 U.S. Dist. LEXIS 153436 (D.D.C. Oct. 29, 2014).

344. *Id.* at *5–6.

345. *Id.* at *15.

346. *Id.* at *17 (citing *White v. Four Seasons Hotels & Resorts*, 999 F. Supp. 2d 250, 257 (D.D.C. 2013)).

347. *Id.* at 18 ("Though YouTube is undoubtedly a popular video-sharing website, it is not the case that Plaintiffs lacked any kind of meaningful choice as to whether to upload their video to the YouTube website and agree to the conditions set forth by YouTube."). Moreover, it was further emphasized that the fact that the users lack bargaining power does not *prima facie* indicate that the contract is unconscionable. In this respect, the court noted that "[a] contract is no less a contract simply because it is entered into via a computer." *Id.* (quoting *Forrest v. Verizon Commc'ns, Inc.*, 805 A.2d 1007, 1011 (D.C. 2002)).

348. According to section 7.8 of YouTube's ToU. *See supra* note 11.

possibility of removing legitimate content that constitutes fair use, through, for example, its Content ID automatic copyright infringement identification system.³⁴⁹ The court firmly denied the plaintiffs' claims, emphasizing that if users "take advantage" of the sharing platforms' "free services," they "cannot complain" that the terms of these platforms are unconscionable.³⁵⁰

In the eyes of the court, so it seems, if you did not pay for the product, meaning you received a free "service," then you are not a consumer under the classic interpretation of this term, and you are unqualified to argue for unconscionability. The court failed to acknowledge that in the era of Web 2.0 and user-generated content, if you do not pay for the product, you—or the IP you create—may very well become the actual product.³⁵¹

349. The contractual consent of the adherent-creator to YouTube's ToU, combined with YouTube's Content ID system, enables YouTube (and alleged owners) to remove legitimate content and expression *ex ante*, rather than relying on the DMCA procedures for removal of infringing content *ex post*. *See* 17 U.S.C. § 512(c)(1)(A) (1998). As Zimmerman argued, "instead of relying on the notice and takedown system, the *ex post* remedy stipulated by the DMCA, YouTube now allows content owners to engage in a priori control of what can appear on the site." Zimmerman, *supra* note 178, at 272. Instead of relying on the legislature, YouTube uses private ordering mechanisms (the IP boilerplate and the Content ID system) to formulate an alternative removal regime. YouTube's motivations for this are clear. First, it allows YouTube to enjoy the protection of the Safe Harbor defense under the DMCA. *See* *Viacom Int'l Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012)). But it also enables YouTube to increase profits when the alleged owner chooses to utilize the "infringing" content as a creative publishing platform rather than silencing it. *See* Zimmerman, *supra* note 178, at 272–73. Arguably, this is one result of the fact that "[f]air use bec[ame] subject to private gain." LESSIG, *supra* note 105, at 135.

350. *Song Fi, Inc. v. Google Inc.*, No. 14-1283 (RMC), 2014 U.S. Dist. LEXIS 153436 at *20 (D.D.C. Oct. 29, 2014) ("[N]one of these terms, nor the contract as a whole, is 'so outrageously unfair as to shock the judicial conscience.' . . . Indeed, courts routinely enforce such terms in form contracts. . . . Unless there is some evidence of 'egregious' tactics, of which there is none here, 'the party seeking to avoid the contract will have to show that the terms are so extreme as to appear unconscionable according to the mores and business practices of the time and place.' . . . Having taken advantage of YouTube's *free services*, Plaintiffs cannot complain that the terms allowing them to do so are unenforceable.") (emphasis added).

351. The saying "if you are not paying for it, you're not the customer; you're the product being sold" is attributed to the blogger blue_beetle. blue_beetle, *User-Driven Discontent*, METAFILTER, (Aug. 26, 2010, 1:41 PM) www.metafilter.com/95152/Userdriven-discontent#32560467 [<https://perma.cc/8FU3-UYEW>]. Similar results were reached in a recent case. *See* *Darnaa, LLC v. Google, Inc.*, No. 15-cv-03221-RMW, 2015 U.S. Dist. LEXIS 161791 (N.D. Cal. Dec. 2, 2015). In *Darnaa*, the plaintiff argued that several provisions of YouTube's ToU, including, *inter alia*, the terms that allow YouTube broad discretion over content removal, are unconscionable. The court found that YouTube's ToU "involve only a marginal degree of procedural unconscionability," and are not "one-sided as to be substantively unconscionable." *Id.* at 8. Moreover, the court emphasized, in the framework of the unconscionability analysis, that "[b]ecause YouTube offers its hosting services at no charge, it is reasonable for YouTube to retain broad discretion over those services. . . ." *Id.*

Arguably, in a world governed by myth of “free,”³⁵² consumers have changed. They are no longer ordinary consumers. They pay a high price for their use of “free” services and platforms—the price of their information, their innovations, and their IP rights. In this respect, even the Restatement puts excessive focus on the issue of the service or product “price” and less on “free” services.³⁵³

Courts clearly are still unequipped to address IP boilerplate under the current interpretation of unconscionability in a manner that regulates IP rights in an *ex-consumerist* setting, but does not involve payment.³⁵⁴ Yet, in reality, popular platforms offer no-cost services, and their use often leads to severe IP problems.³⁵⁵ This issue will be addressed under the proposed

352. See Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606 (2014); John M. Newman, *The Myth of Free*, 86 GEO. WASH. L. REV. 513 (2018).

353. See, e.g., The Restatement, *supra* note 29, at 51. Although it does apply its principles to privacy policies as well, to some extent.

354. Not surprisingly, this narrative is also evident in case law addressing unconscionability claims of adherent-creators in non-virtual realms. See, e.g., *Cubic Corp. v. Marty*, 185 Cal. App. 3d 438, 450 (Cal. App. 4th Dist. 1986) (providing an example of unconscionability claims in employment relationships. The court rejected the claim that the invention assignment provision is unconscionable on the grounds that the “[inventor] was adequately compensated through the terms of his employment.” *Marty*, the inventor, claimed that a payment of \$75.00 was “unreasonably low compensation for the [i]nvention”); see also *Reach Music Publ'g, Inc. v. Warner/Chappell Music, Inc.*, No. 09 Civ. 5580(KBF), 2014 WL 5861984 (S.D.N.Y. Nov. 10, 2014) (providing a more recent example. The matter concerned David Reeves’ rights in some of the famous songs of the band Run-DMC. Reeves, who contributed to the creation of the band’s songs, assigned his rights in them to a distributor in return for royalties’ revenues. Rush Groove, the distributor who later went bankrupt, assigned these distribution rights to Protoons Inc. Alas, according to the terms of the contract, Reeves was only entitled to claim royalties from Rush Groove, which ceased to exist (or pay). Furthermore, Reeves had explicitly waived any right of action against Protoons Inc. Years passed, and while Run-DMC became a resounding commercial success, Reeves became homeless. Reeves claimed, inter alia, that the contract was unconscionable, arguing that when he signed the contract, he had little understanding of the significance of the assignment. He further alleged that he was not provided with a copy of the contract or the opportunity for legal consultation. Reeves did not even pass the hurdle of procedural unconscionability. The court found that “one cannot generally avoid the effect of a release upon the ground that he or she did not read it or know its contents”). The problem is not the specific outcome of these rulings, but the fact that courts are focused *only* on the contractual setting in their analysis of unconscionability and fail to address the relevant purposes of IP laws pertaining to the matter at hand. See GIUSEPPINA D’AGOSTINO, *COPYRIGHT, CONTRACTS, CREATORS: NEW MEDIA, NEW RULES* 72–75, 135–37 (2010) (reporting a similar approach in Canada, in which “courts’ equitable jurisdiction provides the judicial capacity to strike down contracts in whole, or in part, on the basis of unconscionable terms or conduct, though equity has seldom been used”).

355. See, e.g., Elkin-Koren, *Can Formalities Save the Public Domain?*, *supra* note 101, at 1550, 1561.

Unconscionability 2.0. Moreover, the *Song Fi* decision demonstrates that the underutilization of unconscionability is particularly problematic when considering a case involving an adherent-creator type of contract, such as the YouTube ToU, where preemption and misuse are not claimed but unconscionability is.

3. *A Limited Tool Set: From ProCD and Preemption to Lexmark and Exhaustion*

The *Lexmark* case discussed earlier exposes another dimension of inconsistency in how U.S. IP laws treat the IP boilerplate problem and emphasizes the need for a nuanced tool situated between form contracts and IP laws that can also distinguish between contracts. In a concise opinion, the Supreme Court in *Lexmark* articulated a bright-line rule for the patent/contract interaction, without accounting for the nature of the communication involved or distinguishing between standard form and negotiated contracts.³⁵⁶

The Court clarified that “single-use/no-resale restrictions in *Lexmark*’s contracts with customers may have been clear and enforceable under contract law, but they do not entitle *Lexmark* to retain patent rights in an item that it has elected to sell.”³⁵⁷ The Court devoted a kernel of its reasoning to discussing the longstanding common law principle against restraints on alienation and the underpinning principles of the exhaustion rule: a sound public policy principle.³⁵⁸

The Court reasoned that allowing restraints on trade would result in “inconvenience and annoyance to the public.”³⁵⁹ This reflected the Court’s growing concern about creating a legal reality in which “[the] smooth flow of commerce would sputter” since “companies that make the thousands of parts that go into a [product] could keep their patent rights after the first sale . . . restrict resale rights and sue the shop owner for patent infringement,”³⁶⁰ especially in light of advances in technology and the growing complexity of supply chains.³⁶¹

Still, if the legal system strives to eliminate restraints on alienation that grant the patentee unwarranted monopolistic rights and “control” over the patent, why should courts enable a contractual claim that arises from such restrictions and might result in the same “clog” of commerce channels? Should

356. *Impression Prods. v. Lexmark Int’l, Inc.*, 137 S. Ct. 1523 (2017).

357. *Id.* at 1531.

358. *Id.* at 1534 (“A patentee can impose restrictions on licensees because a license does not implicate the same concerns about restraints on alienation as a sale.”).

359. *Id.* at 1532 (quoting *Keeler v. Standard Folding Bed Co.*, 157 U.S. 659, 667 (1895)).

360. *Id.*

361. *Id.*

this result be allowed just because such restraints generate a different type of suit (a contractual one as opposed to a patent one) to fear?

The core logic of exhaustion limits “the scope of the patentee’s rights” and “extinguish[es] that exclusionary power.”³⁶² In the information age, IP boilerplate is often used for wholesale “contracting” of such post-sale restrictions that share the same characteristics of traditional servitudes and restraints on alienation, which creates similar exclusionary rights.

Almost a decade ago, Van Houweling demonstrated how contemporary licensing practices operate similarly to servitudes³⁶³ and create the same challenges with which the *Lexmark* Supreme Court is concerned: notice and information costs and negative externalities.³⁶⁴ IP boilerplate, like servitudes, often enforces restrictions that are nonsalient or ubiquitous across entire markets, meaning they are not subjected to competitive market forces that regulate the quality of the terms.³⁶⁵ IP boilerplate creates a similar shade and “legal cloud on [a] title as [it] move[s] through the marketplace” that exhaustion seeks to eliminate.³⁶⁶

These boilerplate, as opposed to the utopian license envisioned by the Court, often do not seek to “expand the club of authorized producers and sellers” but rather to limit them or the ability of the licensee, often a consumer, to otherwise use the patent. They are used in the exchange of goods and are not merely rights.³⁶⁷ If the Court is truly motivated by the common law’s longstanding resistance toward restraints on alienation, not enabling post-sale restrictions under patent law does not solve the issue of boilerplate-based contractual restrictions, which generate the very same concerns. The Court discounts such concerns, stating that “a license does not implicate the same concerns about restraints on alienation as a sale,”³⁶⁸ but such a statement is somewhat detached from the reality of mass-market licenses.

362. *Id.* at 1534.

363. *See* Van Houweling, *supra* note 80, at 903 (clarifying that not all servitudes are concerned with restraints on alienation).

364. *Id.* at 949–50 (“[T]hese concerns arise from specific characteristics of servitudes including: the remote relationship between the burdened and benefited parties, the durability and ubiquity of the restrictions imposed, the fragmentation of rights to control use of a single resource, the potential lack of salience to purchasers, and the insulation from effective competition where servitudes are attached to goods with unique qualities or are ubiquitous across entire markets. . . . [E]ach of the paradigmatic licenses that I have examined exhibits a different mix of problematically servitude-like features.”).

365. *Id.*; *see also* Korobkin, *supra* note 74.

366. *Impression Prods. v. Lexmark Int’l, Inc.*, 137 S. Ct. at 1531, 1534.

367. *Id.*

368. *Id.*

In that respect, both the en banc decision³⁶⁹ and the Supreme Court decision missed a unique opportunity to clarify the essence of the sale/license dichotomy and limit the servitude-like costs associated with IP boilerplate. As mentioned, it is well established that the patentee can impose contractual restrictions on secondary markets, but she cannot use patent law for that purpose.³⁷⁰ Among the cases in which this was established is a 1938 Supreme Court exhaustion case, *General Talking Pictures*, which greatly influenced the en banc *Lexmark* decision. Yet *General Talking Pictures* specifically distinguished the circumstances of the case from those discussed in *Lexmark*, in which the post-sale restrictions are communicated to consumers on labels or other forms of “take-it-or-leave-it” adhesive contracts used in ordinary commerce, but where actual knowledge is not guaranteed.³⁷¹

Ordinary consumers have no incentive to read the fine print, and as discussed, empirical research in fact shows they almost never do so. Regardless, *General Talking Pictures*, even under the Supreme Court *Lexmark* decision, continues to guide courts and provide supportive reasoning for the purpose of answering the exact question the court then explicitly avoided: how to determine the enforceability of wholesale post-sale contractual restrictions on licensees under patent law. Using Van Houweling’s framing, the Federal Circuit in *Lexmark* took a case where the informational burden was limited,³⁷² and applied its reasoning to a general case where information costs constrain ordinary consumer behavior.³⁷³ The Federal Circuit, though it had the opportunity, did not differentiate between the actual knowledge that the manufacturing licensee had, such as in *General Talking Pictures*, and the knowledge that ordinary consumers, such as *Lexmark*’s consumers, usually have.

369. See *Lexmark Int’l, Inc. v. Impression Prods.*, 816 F.3d 721 (Fed. Cir. 2016).

370. See *Keeler v. Standard Folding Bed Co.*, 157 U.S. 659, 666 (1895); *Quanta Comput., Inc. v. LG Elecs., Inc.*, 553 U.S. 617, 638 (2008).

371. There is no dispute that the “package restriction” discussed in *Lexmark* is an adhesion contract, which is offered to consumers on a “take-or-leave-it” basis. In fact, the *Lexmark* “single-use” label restriction was explicitly challenged in U.S. case law prior to this patent case. Courts enforced these restrictions under contract law, albeit emphasizing that these are adhesion contracts. Accordingly, the fact that the *Lexmark* “patent-wrap” label agreement (as I call it) was an enforceable agreement was undisputed in the present decision. See *Lexmark*, 816 F.3d at 728.

372. See Van Houweling, *supra* note 80, at 920 (providing a case “in which the chattel purchaser [the manufacturing-licensee, Pictures Corporation] could not plausibly claim that it (or any other purchaser similarly situated) could have been confused by, inattentive to, or otherwise cognitively burdened by the existence of a running restriction on its ability to use its personal property”).

373. *Id.*

Moreover, the majority in the *Lexmark* en banc decision specifically noted that the opinion does not address situations where end-users, bona fide purchasers, or downstream re-purchasers “acquired a patented article with less than actual knowledge of such a restriction.”³⁷⁴ Nor did courts address this issue in the *Mallinckrodt* or *Quanta* decisions,³⁷⁵ or in the Supreme Court *Lexmark* decision.

The *Lexmark* en banc decision did not pay much attention to the enforceability of Lexmark’s restrictions from the contractual perspective, since this matter was supposedly already settled in *Static*.³⁷⁶ Although the court in *Static*³⁷⁷ compared Lexmark restrictions to the *ProCD* shrinkwrap license and found it enforceable,³⁷⁸ the court did not address more important questions of exhaustion and effects on public policies. Courts have yet to solve the problem of non-negotiated licenses that merely provide notice of such restrictions, where actual knowledge is not proven and informational costs exist.

And thus, a *ProCD*-moment in time was missed—a moment in which the Court could have clarified how much room is given to form contractors to displace IP policy. Currently, at least according to the recent *Lexmark* Supreme Court decision, exhaustion will fail to curtail the various costs associated with mass-market unnegotiated contractual restrictions attached to innovations. The post-sale restrictions will remain enforceable (or at least are not unenforceable) under contract law. At least one conflicting decision has already used misuse, in the context of copyright, to arrive at a different result where the contract could not be enforced.

Yet exhaustion in the *Lexmark* case cannot provide a contextualized solution to the intuition that we should differentiate between actual knowledge and “presumed” knowledge of restrictions communicated by notice. It also cannot account for the “servitude-like” costs associated with wholesale standardized restrictions. The reason is that exhaustion does not, and is not

374. *Lexmark*, 816 F.3d at 729. The parties agreed that “both the first purchaser and Impression as a repurchaser had adequate notice of the single-use/no-resale restriction before they made their purchases” and therefore “the adequacy of that notice [was] unchallenged.” *Id.*

375. *Mallinckrodt, Inc. v. Medipart, Inc.*, 976 F.2d 700, 708 (Fed. Cir. 1992).

376. *Lexmark*, 816 F.3d at 728.

377. *See, e.g.*, *Static Control Components, Inc. v. Lexmark Int’l, Inc.*, 487 F. Supp. 2d 830, 845 (E.D. Ky. 2007) (citing *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996)) (enforcing Lexmark’s labels under contract law, albeit emphasizing these are adhesion contracts offered to consumers on a “take-or-leave-it” basis and further comparing them to the notorious “shrinkwrap licenses,” “in which a vendor’s written license becomes ‘effective as soon as the customer tears the wrapping from the package’”). Shrinkwrap licenses in which consumers “Pay Now” but see the “Terms Later” are enforceable contracts in the United States following *ProCD*.

378. *Id.* at 845, 847.

geared to, differentiate between negotiated and standard form contracts.

It is the very fundamental features of standardized contracts (as opposed to negotiated ones) that often give rise to the “servitude-like” notice and informational costs.³⁷⁹ And not all standard form contracts raise the same concerns.³⁸⁰ Exhaustion must operate as a clear rule as to where that owner’s monopolistic rights and her ability to bring a patent infringement suit ends. That is the point of the first sale. This does not mean the exact same normative results are warranted for negotiated and unnegotiated contracts.

Conversely, in these situations, Unconscionability 2.0 offers a unique contribution. It is the intersection between standard form contracts and IP laws that created the problem, and therefore both disciplines must inform a tool that solves it. Indeed, exhaustion, like preemption and misuse, is not geared to inquire into the salience of terms—but unconscionability is. The unconscionability inquiry traditionally did not account for the harmful externalities that may be caused to society by such restrictions from an IP perspective.³⁸¹ But Unconscionability 2.0 can.

Today’s commercial world has long departed from a reality where restrictions on licensees attached to innovations are only bargained for, and contracted with, well-informed manufacturing licensees, as was envisioned by early exhaustion cases such as *United States v. General Electric Co.*,³⁸² *Motion Picture Patents Co. v. Universal Film Manufacturing Co.*,³⁸³ and *General Talking Pictures Corp. v. Western Electric Co.*³⁸⁴ It now includes licenses that “govern” (as opposed to contract with) consumers who have very limited information about the post-sale or usage restrictions attached to the product or any incentive to learn about them. The transaction between the manufacturing-licensee and the patentee, as opposed to the one with consumers, will necessarily be “information-intensive.”³⁸⁵ Therefore, we need a tool that accounts for that shift, since exhaustion, as the *Lexmark* Supreme Court decision might suggest, does not. Enter Unconscionability 2.0.

Moreover, drawing some commonalities between the *Lexmark* en banc decision (and exhaustion) and *ProCD* (and preemption) helps to illuminate why we need a doctrine such as Unconscionability 2.0 that allows for

379. *Id.* at 933.

380. *Id.* at 935–37 (explaining how the GPL and Creative Commons licenses, standardized contracts by all accounts, do not exhibit the same notice and information cost concerns as the Microsoft EULA).

381. *See id.* at 331 (“[T]hird-party harm could arise from the enforcement of restrictions that effectively waive public-regarding limitations built into intellectual property law.”).

382. *United States v. Gen. Elec. Co.*, 272 U.S. 476 (1926).

383. *Motion Picture Patents Co. v. Universal Film Mfg. Co.*, 243 U.S. 502 (1917).

384. *Gen. Talking Pictures Corp. v. W. Elec. Co.*, 305 U.S. 124 (1938).

385. Van Houweling, *supra* note 80, at 917.

contextualization and accounts for different types of contracting mechanisms and the costs associated with them. Two decades ago, the Court of Appeals for the Seventh Circuit faced a similar situation as the Federal Circuit in *Lexmark*, where the court had the unique opportunity to establish how IP owners would be able to restrict the manner in which consumers who purchase software products use such products.

Although the *ProCD*³⁸⁶ case involved copyrighted works and was framed around preemption,³⁸⁷ at least two important commonalities exist between *Lexmark* and *ProCD*. First, in both cases, the owner tried to use contractual limitations in order to bypass the IP regime and limit the user from doing something that was explicitly permitted under IP law. In *ProCD*, it was harvesting data not protected under copyright law (phone records). In *Lexmark*, it was the post-sale restriction. Second, in both cases, the owners of the IP-protected products offered the consumers a choice. In *Lexmark*, consumers could choose between buying regular cartridges and the return-program cartridges, which cost 20% less but were subject to the single-use restriction. In *ProCD*, the owner offered the software at two prices: one for personal use and a higher price for commercial use. In both cases, the court used this fact to justify why IP owners should be able to contractually limit consumers from doing something that IP legal doctrine explicitly deems lawful.³⁸⁸ The *ProCD* and *Lexmark* circuit courts both believed that benefits that stem from this commercial conduct surpass the importance of the IP legal doctrine discussed. Twenty years have passed since *ProCD* and we now know that the *ProCD* holding is being used for a wide range of circumstances that do not involve consumer choices.³⁸⁹ The Supreme Court had a chance to clarify, at least in dictum, the question of contractual enforcement of post-sale restrictions in consumerist settings and it did not do so.

The *Lexmark* en banc decision was not limited to cases in which consumers presumably have a choice—and inevitably, if that holding survives Supreme Court review, post-sale restrictions may expand to all commercial relations, including perhaps even products that are “free,” pending users’ assent.

The majority in the *Lexmark* en banc decision found that no reliable evidence was given as to the widespread problems that post-sale restrictions could pose, problems that are not “solved in the marketplace.”³⁹⁰ However, twenty years of experience with *ProCD* has demonstrated how contractual

386. *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

387. 17 U.S.C. § 301(a) (2018).

388. If they breach such limitations, consumers could be sued for contract infringement under *ProCD*, and for patent infringement under the *Lexmark* en banc decision.

389. See Rub, *Copyright Survives*, *supra* note 36.

390. *Lexmark Int’l, Inc. v. Impression Prods.*, 816 F.3d 721, 752 (Fed. Cir. 2016).

restrictions may limit users' rights to fair use and access to creative building blocks³⁹¹—regardless of the price charged (or not). Often these restrictions do not translate automatically to an “immediate up-front benefit.”³⁹² Instead, they impose costs—on the specific user, and on society as a whole—and they serve to further perpetuate the permission culture in IP realms. Both courts erred in making a general decision about the appropriate boundaries of the relevant IP doctrine that affected how private ordering, and specifically standard form contracts, may rewrite IP laws.

This can be traced to courts' willingness to generally allow negotiated contracts, which will facilitate price discrimination and enable the owner to control arbitrage that contributes to market efficiency.³⁹³ But in reality, the courts did not account for the contracts' economic and societal costs in a world flooded by unnegotiated standard form contracts and inhabited by real consumers. These consumers value a limited number of the product attributes, and such contractual restrictions are usually not among them. Thus, drafters (or patentees in our case) have an inherent “market incentive to include terms . . . [that] favor themselves, whether or not such terms are efficient.”³⁹⁴ In simple terms, since post-sale “fine print” restrictions will not affect the price, there will be no market competition over these restrictions.

These sorts of market failures, which relate to the bounded rationality of consumers and asymmetric information regarding a key feature of the product such as a post-sale use/re-sale restriction, prevent the patent from being adequately valued in the marketplace. Consumers often struggle to adequately differentiate between a sale and a license, especially when they buy a tangible good, and receive mixed signals from the seller.³⁹⁵ These will be the considerations at hand when the question of the contractual enforcement of post-sale restrictions in form contracts will, inevitably, be raised once again. While *Lexmark* was clearly a sale, a more indistinct case would require courts to inquire what the consumers' expectations and perceptions of their rights

391. See, e.g., the discussion in the *Baystate* and *Davidson* cases, under Section III(B)(ii) “The Preemption Doctrine and the Contract-IP ‘Dichotomy’ ” (enforcing the contractual waiver of a fair use, reverse engineering, communicated to consumers in a standard form contract).

392. *Lexmark*, 816 F.3d at 752.

393. See, e.g., *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1450, 1454–55 (“[T]erms and conditions offered by contract reflect private ordering, essential to the efficient functioning of markets.”); *Lexmark*, 816 F.3d at 752; see also Brief of 44 Law, Economics and Business Professors as Amici Curiae in Support of Respondent, *Impression Prods., Inc. v. Lexmark Int'l, Inc.*, 137 S. Ct. 546 (2016).

394. See Korobkin, *supra* note 74.

395. Cf. Perzanowski & Hoofnagle, *supra* note 87, at 320 (providing an example in the context of digital media, as opposed to physical products: “[w]hile lawyers might comprehend the difference between a license and a traditional sale, there are good reasons to doubt that the average consumer appreciates this distinction”); see also *id.* at 327–30.

were, perhaps even taken into account empirical evidence.³⁹⁶

In some respects, this was a result of the limited toolset available to the courts in *ProCD* and *Lexmark*. Both preemption (under the existing interpretation) and exhaustion allow only for a binary result: either we allow contracts to override the relevant limitations on monopolistic rights that the IP regime imposes, or we do not. Courts do not have the ability to screen the type of contract at issue; therefore, they are forced to use the tools they have to reach their conclusions. Misuse allows for some more discretion, but its results remain scattered. A more nuanced tool such as Unconscionability 2.0 can allow such contextualization, thus enabling courts to reach different results according to the contract at hand, and distinguishing negotiated contracts from unnegotiated ones, while accounting for the salience of terms and inquiring whether the market can solve the problem.

4. *The Dialogue of the Deaf*

IP scholars were not the only ones concerned about IP boilerplate; contract law scholars also began studying the prevalent phenomenon of software licenses, and the empirical literature in this field actually focuses on the consumer perspective.³⁹⁷ Marrota-Wurgler, for example, examined 647 end-user licenses drafted by 598 software companies in different market segments.³⁹⁸ The study proposed using the “Bias Index,” by which the usage frequency of some twenty-three recurring provisions was mapped as benefiting the user, or alternatively, the supplier. The benchmark used was the standards incorporated under the Article 2 of the U.C.C. default rules. The conclusions of Marrota-Wurgler’s study indicated that the contracts were characterized by a unilateral bias in favor of the supplier.³⁹⁹

396. The Restatement, *supra* note 29, at 82; *see also* Omri Ben-Shahar & Lior Jacob Strahilevitz, *Interpreting Contracts via Surveys and Experiments*, 92 N.Y.U. L. REV. 1753, 1753 (2017) (proposing the “survey interpretation method”—“in which [contract] interpretation disputes are resolved through large surveys of representative respondents, by choosing the meaning that a majority supports”).

397. Paradoxically, despite the growing prevalence of such contracts, there is still little legal empirical literature at hand. *See* Eyal Zamir & Yuval Farkash, *Standard Form Contracts: Empirical Studies, Normative Implications, and the Fragmentation of Legal Scholarship*, 12 JERUSALEM REV. LEGAL STUD. 137, 148 (2015) (providing further criticism); *see also* Florencia Marotta-Wurgler, *What’s in a Standard Form Contract? An Empirical Analysis of Software License Agreements*, 4 J. EMPIRICAL LEGAL STUD. 677, 678 (2007) [hereinafter Marotta-Wurgler, *What’s in a Standard Form Contract?*].

398. Marotta-Wurgler, *What’s in a Standard Form Contract?*, *supra* note 397, at 679.

399. *Id.* at 713 (“An immediate conclusion is that the vast majority of the contracts in our sample are more pro-seller relative to the default rules of Article 2 of the UCC.”).

The most interesting insight is that no correlation was found between the price of the product and the severity of the bias in favor of the supplier,⁴⁰⁰ which leads to the conclusion that there is no connection between the price of the product and the clear preferences of the consumers.⁴⁰¹ An additional study that examined the browsing pattern of nearly 50,000 users revealed that only 1 to 2 per 1,000 users browses through the Internet page displaying the end-user license for longer than one second.⁴⁰² This study proved that in practice, consumers do not read these contracts, thus empirically rejecting the “informed minority” argument of the economic school of contract law analysis.⁴⁰³ It essentially proved the nonsalience of EULA terms, and the inevitable conclusion is that the de facto informed minority cannot affect the willingness of suppliers to change the contract terms in real market conditions.⁴⁰⁴

A series of additional empirical studies led Marrota-Wurgler to the conclusion that there is no point to the significant disclosure requirements pertaining to EULAs;⁴⁰⁵ on the contrary, such requirements only burden the

400. *Id.* at 708.

401. Zamir & Farkash, *supra* note 397, at 139–40.

402. Bakos et al., *supra* note 28, at 3.

403. According to that argument, a minority of consumers who do read the terms and conditions is sufficient for the suppliers to adjust themselves to consumers’ preferences in view of the market forces—hence the market will in any event create fair contracts and no external juridical interference is required. *See* Alan Schwartz & Louis Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630 (1979). Since the supplier is not able to distinguish between this informed minority and the uninformed majority of consumers, it will offer all consumers identical terms. *See* Howard Beales et al., *The Efficient Regulation of Consumer Information*, 24 J.L. & ECON. 491 (1981); ELENA D’AGOSTINO, *CONTRACTS OF ADHESION BETWEEN LAW AND ECONOMICS RETHINKING THE UNCONSCIONABILITY DOCTRINE* 62 (2015). One scholar, Moffat, specifically rejected the application of the informed minority argument in the context of contractual fair use limitations. She noted that even the informed minority (the so-called “readers”) “are unlikely to negotiate or shop for super-copyright provisions because the provisions generally are too minor on an individual basis—their effects are problematic in the aggregate” and that “[t]o the extent that the behavior of the readers influences the behavior of the non-readers, the effects will only be compounded.” Moffat, *supra* note 43, at 56–57.

404. Bakos et al., *supra* note 28, at 3.

405. Florencia Marotta-Wurgler, *Even More Than You Wanted to Know About the Failures of Disclosure*, 11 JERUSALEM REV. LEGAL STUD. 63, 65 (2015). This is the result, inter alia, of extensive disclosure requirements imposed on drafters. These requirements, which were perceived as an effective solution to information asymmetry, paradoxically contributed to the problem. *See id.* at 65 (“[I]ncreases in disclosure may have allowed firms to put forth more restrictive contracts and, at the same time, enforce them more effectively.”); *see also* Florencia Marotta-Wurgler, *Are “Pay Now, Terms Later” Contracts Worse for Buyers? Evidence from Software License Agreements*, 38 J. LEGAL STUD. 309 (2009) [hereinafter Marotta-Wurgler, *Are “Pay Now,*

users and confuse them, and thus the focus should be on whether terms are an appropriate outcome of competitive market forces.⁴⁰⁶

These ideas have been extensively researched by Ben-Shahar and Schneider, who surveyed empirical findings from various sectors—ranging from food labels to credit terms—and reached the conclusion that “the empirical history of mandated disclosure is a history of failure.”⁴⁰⁷ It follows from the conclusions of contractual-consumerist studies at the forefront of the literature⁴⁰⁸ that despite the many words written about the lack of necessity of interference in boilerplate enforcement, the empirical reality proves otherwise, and it is time to find new doctrinal solutions.⁴⁰⁹ Economists recognized that since consumers have bounded rationality, they often don’t translate the quality of the contract terms to the price.⁴¹⁰ This focus on the efficiency of courts’ interference in the case of nonsalient terms influenced the Restatement, and is key in the case of understanding terms pertaining to IP rights, which are more complex, especially for ordinary consumers.⁴¹¹

In a recent empirical research done by Hoofnagle and Perzanowski,⁴¹² the authors found not only that merely a minority of consumers read the terms, but that online digital media consumers are often confused about whether they are actually buying the product or licensing it, and which IP and property

Terms Later” Contracts Worse for Buyers?]; Florencia Marotta-Wurgler & Robert Taylor, *Set in Stone? Change and Innovation in Consumer Standard-Form Contracts*, 88 N.Y.U. L. REV. 240 (2013).

406. See Marotta-Wurgler, *Are “Pay Now, Terms Later” Contracts Worse for Buyers?*, *supra* note 406, at 431; see also Shmuel I. Becher & Tal Zarsky, *Online Consumer Contracts: No One Reads, But Does Anyone Care: Comments on Florencia Marotta-Wurgler’s Studies*, 12 JERUSALEM REV. LEGAL STUD. 105, 120 (2015) (reaching the same conclusion).

407. See Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 746 (2011); OMRI BEN-SHAHAR & CARL E. SCHNEIDER, *MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE* (2014). According to the authors, this is a three-fold failure: (i) even if disclosure of information is required, in reality consumers don’t receive the information; (ii) consumers don’t read the disclosed information, and even if they do—they often don’t understand it, and if they understand it—they don’t use it; and most importantly, (iii) disclosure does not improve consumers’ decision-process making. *See id.* at 665.

408. Zamir and Farkash, for example, presented Marotta-Wurgler’s empirical scholarship as “arguably the most important contribution to contract law theory in the past decade.” Zamir & Farkash, *supra* note 397, at 138.

409. *Id.* at 170.

410. See Korobkin, *supra* note 74; see also Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 545 (2014) (“Instead of promoting informed consumer assent through quixotic attempts to have consumers read ever-expanding disclosures . . . consumer protection law should focus on ‘term optimism’-situations in which consumers expect more favorable terms than they actually receive.”).

411. Elkin-Koren, *Contracting Copyrights*, *supra* note 2, at 200.

412. Perzanowski & Hoofnagle, *supra* note 87.

restrictions apply to the product.⁴¹³ In addition, Hoofnagle and Perzanowski found that simplified disclosure mechanisms enhance consumers' comprehension of the rights they obtain under the restrictive license language used in digital media transactions.⁴¹⁴ Moreover, the authors argue that lowering the information costs associated with rights understanding could promote competition with respect to the licensed rights.⁴¹⁵ Similar results were reached in other empirical studies, dating as far back as 2007, showing that providing a simplified notice on EULA rights (prior to installation, and after installation, allowing a user to uninstall the program) will reduce the number of software installations in a significant manner, meaning it will increase terms' salience (affecting users' decision-making).⁴¹⁶ This is an example of inter-doctrinal research which seeks to address consumer law, as well IP-related concerns.

An additional explanation for the underutilization of the unconscionability doctrine could be inferred from the above discussion. The problem begins with the sometimes inefficient dialogue between the IP and contract scholars who explore the IP boilerplate problem. Contract scholarship often lacks the required attention to the nature of the contract at hand as one that seeks to regulate IP rights. This naturally derives from the consumerist perspective from which these contracts are viewed—and the fact that the focal point for analysis of these adhesive terms is rooted in the U.C.C.⁴¹⁷ This further affects the perception of the entire unconscionability doctrine.

Interestingly enough, this “dialogue of the deaf” led a number of IP commentators to propose solutions that are based on “clear

413. *Id.*

414. *Id.* at 349–50.

415. *Id.* at 376 (“[L]owering the information costs associated with understanding the rights consumers acquire, short notices might create incentives to offer more attractive bundles of rights.”).

416. *See id.*; *see also* Nathaniel S. Good et al., *Noticing Notice: A Large-Scale Experiment on The Timing of Software License Agreements*, 2007 PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS ACM 612. Yet the researchers still found that even users that installed the software regardless of the EULA notice regretted it later on in the process. *Id.* at 614.

417. U.S. courts have considered a transaction involving a software license to be a sale of goods, often looking to the U.C.C. for answers to questions related to contract enforcement. As Marotta-Wurgler argues,

Numerous courts have held that the sale (or licensing) of software should be interpreted as the sale of a good within the meaning of the U.C.C. Consequently, when faced with a dispute over the validity of a software EULA or a particular term contained therein, courts have relied on Article 2 of the U.C.C. (and relevant U.C.C. Article 1 provisions) to determine its enforceability.

Marotta-Wurgler, *What's in a Standard Form Contract?*, *supra* note 397, at 690.

communication”⁴¹⁸ and disclosure⁴¹⁹ in order to mitigate some of the problems created by IP boilerplate, although empirical contractual-consumerist research indicates that such disclosure is not necessarily effective.

As I explained in the previous Section, boilerplate, by definition, will almost never give raise to “actual knowledge.” Nor is it an adequate tool to “clearly communicate.” The rationale for imposing the “clearly communicated” threshold and the “actual knowledge” requirement cannot be reconciled with the fact that according to the majority in the en banc *Lexmark* decision, the enforceability of these “otherwise-lawful” post-sale resections should be decided, inter alia, as a matter of contract law.⁴²⁰

IV. UNCONSCIONABILITY 2.0—TOWARDS A REVISED DOCTRINE OF UNCONSCIONABILITY DERIVED FROM INTELLECTUAL PROPERTY RATIONALES

In this Article, I focus on a new legal phenomenon that has emerged in today’s information society: the rise of the IP boilerplate. These contracts seek to regulate, control, and appropriate intellectual products, content, resources, and expressions. While “traditional” boilerplate raises fundamental questions concerning consumer and contract laws, IP boilerplate raises questions deeply rooted in the core of IP law—from regulating user rights to the legal status of students’ creations and employees’ inventions. Thus far it has been argued that while the problems created by these contracts have long been recognized by scholars, unconscionability was unjustly overlooked as a potential inter-doctrinal solution. Indeed, “while [the] tension [between contracts and copyright law] can, at least in theory, be addressed using various doctrinal vehicles . . . under state contract law, in practice, it has almost exclusively been

418. See Brief of 44 Law, Economics and Business Professors as Amici Curiae in Support of Respondent, *Impression Prods., Inc. v. Lexmark Int’l, Inc.*, 137 S. Ct. 546 (2016) (No. 15-1189).

419. See, e.g., Lisamarie A. Collins, *Copyrightable Works in the Undergraduate Student Context: An Examination of the Issues*, 17 MARQ. INTELL. PROP. L. REV. 285, 297 (2013). Collins addressed the problem of students who are required to assign all rights in their creations pursuant to an academic institution’s standard policies. Collins agreed that such assignment might be held unconscionable, yet she offered legislative and disclosure-based solutions to accommodate the problem. *Id.* at 302 (“If legislative action is not feasible, then universities, at minimum, should seek to inform students as early as possible of their intellectual property policies . . .”). Although students are not typical consumers, experience shows that they too are often unaware of their rights, and they avoid reading browsewrap. See, e.g., Amit Elazari, *Position Paper: The Legal Status of Students’ Intellectual Property Rights in Academic Design Institutions* (Oct. 2012), <http://din-online.info/pdf/std7.pdf> [<https://perma.cc/ND9W-GJFE>] (in Hebrew).

420. *Lexmark Int’l, Inc. v. Impression Prods.*, 816 F.3d 721, 735 (2016).

discussed under the auspice of copyright preemption doctrine.”⁴²¹

I have thus far tried to explain how this result has come about and devoted much of the discussion to the various facets of the problem—I shall now turn to the solution.

According to this solution, Unconscionability 2.0, IP boilerplate should be examined by the unconscionability doctrine, but through the prism of IP theories, as their essence is to regulate IP rights. I suggest that the critical question of whether or not a provision is unconscionable should be examined under a substantive analysis, by asking, generally, if the provision benefits the purposes of the relevant IP policies, or does it, in fact, negate them.

This solution originates in the Israeli purposive interpretation to unconscionability—an approach that led Israeli courts, in the one case in which they were required to do so, to recognize the doctrine as a versatile, pragmatic solution and to analyze IP boilerplate via unconscionability—but strictly by way of examining the purposes of the relevant IP laws to the term in question. In so doing, the Israeli courts achieved something that many U.S. courts have failed to achieve. Adopting this purposive approach will allow us to discard the literal consumer-oriented interpretation of the doctrine, which is clearly ill-equipped to accommodate the challenges presented by the information age. In the following Sections, I will explain the advantages of this Israeli purposive interpretation of unconscionability and address how Unconscionability 2.0 could be reconciled with the Restatement, the current U.S. approach to unconscionability, as well as with the doctrine’s origins. I will further lay a more robust vision for Unconscionability 2.0, and suggest mechanisms to increase its clarity and certainty, such as presumptions of unconscionability. Then I will discuss the application of Unconscionability 2.0 through case studies. Next, I will discuss the application of Unconscionability 2.0 to technological boilerplate in negotiated contracts in various other case studies. I conclude this Part by addressing some critiques of Unconscionability 2.0.

A. THE PROPOSED DOCTRINE OF UNCONSCIONABILITY 2.0

1. *Theoretical Background and Comparative Insights: Adopting a Purposive Approach to Unconscionability*

The Section focuses on the purposive development of the Israeli unconscionability doctrine. While U.S. law remained focused on protecting the narrow financial-consumerist interests of the contractual parties, the Israeli doctrine was liberated from this burden by a series of precedents by former Supreme Court President Barak that adopted the purposive approach. This

421. Rub, *A Less-Formalistic Copyright Preemption*, *supra* note 37, at 338.

interpretation has enabled Israeli courts to utilize the doctrine as a purposeful solution applicable to diverse relationships, not only those that are consumer based, and to accommodate a wide range of non-contractual notions within the boundaries of unconscionability.

The first Israeli law that pertains to this issue was the “Standard Contracts Law” of 1964,⁴²² which applied only to consumer transactions.⁴²³ Before then, boilerplate was addressed under general contract laws.⁴²⁴ The 1964 law enabled courts and the “Board”⁴²⁵ to invalidate unconscionable terms in standard form contracts. This law met great scholarly resistance.⁴²⁶ By the end of the 1970s, it was found that only one provision in a single standard form contract had been invalidated by the application of the 1964 law.⁴²⁷ Alas, this avant-garde law, originally considered as a pioneering legal novelty unheard of in global

422. THE ISRAELI STANDARD CONTRACTS LAW, 5724–1964, (1964) § 18 LSI 51; *see generally* Aubrey L. Diamond, *The Israeli Standard Contracts Law, 5724–1964*, 14 INT’L & COMP. L.Q. 1410 (1965) (providing a general review); *see also* Kenneth Frederick Berg, *The Israeli Standard Contracts Law 1964: Judicial Controls of Standard Form Contracts*, 28 INT’L & COMP. L.Q. 560 (1979).

423. The legislative history of this law reveals that in the discussions preceding the law’s enactment, the U.C.C. doctrine of unconscionability was viewed as similar to the Israeli unconscionability doctrine under the proposed bill. *See* Sinai Deutch, *Standard Contracts Act: Failure and Recommendation*, 1 BAR-ILAN L. STUD. 62, 126 (1980) (in Hebrew) [hereinafter Deutch, *Standard Contracts Act*]; *cf.* Sinai Deutch, *Controlling Standard Contracts—The Israeli Version*, 30 MCGILL L.J. 458, 569 (1984) [hereinafter Deutch, *Controlling Standard Contracts*]. *See also* Berg, *supra* note 422, at 562 (“In her preparation of the I.S.C.L. [the law], Israel drew upon the limited experiences of other countries, notably the United States, Great Britain and Italy.”).

424. For example, through the Israeli doctrines of public policy and good faith. *See* CA 461/62 Zim Israeli Navigation Co. Ltd. v. Maziar 17 PD 1319 (1963).

425. The Board, which eventually evolved into the Standard Contracts Tribunal, is a designated tribunal—a “control system”—that allows drafters to submit standard form contracts for pre-approval. If the terms are found reasonable, the contract will be “immune” from future judicial intervention. *See* Deutch, *Controlling Standard Contracts*, *supra* note 423, at 473; *see also* Diamond, *supra* note 422, at 1415.

426. Critics argued that the legal outcome resulting from the 1964 law, namely, that standard form contracts that are not intended for the purpose of supplying a commodity or service are excluded from the law, had rendered the law generally inapplicable and redundant. This result, clearly incongruent with the legislature’s original intentions, has forced courts to inquire whether the contract in question is indeed a contract for the supply of a commodity or service in order to apply the law. *See* Deutch, *Controlling Standard Contracts*, *supra* note 423, at 466.

427. CA 280/71 Gideon v. Kadisha Soc’y 27(1) PD 10 (1972) (ruling unenforceable a provision restricting consumers from including the Georgian dates of the birth and death of their loved ones on tombstones purchased from Kadisha on the grounds of unconscionability). Interestingly enough, what became arguably one of the most prominent precedents in Israeli Standard Form Contracts law also involved the adherents’ right to honor the memory of their loved ones by including Georgian dates and Latin characters on tombstones. *See id.*

terms,⁴²⁸ had been narrowly interpreted by the Supreme Court and was eventually disregarded.⁴²⁹

The question of unconscionability was reduced to a formalistic and conservative analysis that considered only two questions, limited in scope: (i) does the term in question constitute a waiver that exempts the supplier from liability for bodily injury?; and (ii) does the supplier hold a monopolistic power and provide a vital service?⁴³⁰ Even though the law's failure was generally attributed to the ineffective enforcement of its provisions, Deutsch noted that, in his view, the law's ineffectiveness stemmed from a reluctance to deviate from the legal rules of traditional contract laws, and from the difficulty of altering legal perspectives to accommodate such deviation. In his view, those responsible for the law's enforcement failed to fully understand the philosophy that produced this avant-garde act and had never actually agreed with such philosophy, inevitably leading to this unfortunate outcome.⁴³¹

Past experience with the flawed application of the Standard Contracts Law of 1964 shows that sometimes courts issued rulings that actually counteracted the purpose of the law, rendering seemingly powerful tools, such as unconscionability, ineffective. This is the state of affairs in the United States today, where the debate over unconscionability remains fixated on consumer-oriented perceptions that originated in the age of traditional standard form contracts, which dealt mostly with traditional services, banking, and physical commodities.⁴³² The doctrine was developed in too narrow a fashion and was not adaptable to changes in the settings and environments that pertain to the evolution of IP boilerplate. On the other hand, when the shortcomings of the 1964 law and the doctrine of unconscionability were finally acknowledged by

428. Eyal Zamir, *Contract Law and Theory: Three Views of the Cathedral*, 81 U. CHI. L. REV. 2077, n.56 (2014) (describing the 1964 law as the “the first of its kind in the world”); *see also* Deutch, *Controlling Standard Contracts*, *supra* note 423, at 460; *cf.* Berg, *supra* note 422, at n.5 (“The Israeli Parliament was a pioneer by its early efforts.”); *see also id.* at 561 (“The Israeli Standard Contracts Law 5724-1964 . . . creatively combined judicial and administrative controls to adjust the imbalances which result from the superior position of the stipulating party.”).

429. *See* Deutch, *Controlling Standard Contracts*, *supra* note 423, at 461 (“Two decades of conservative interpretation by the courts almost reduced the statute to a ‘dead letter.’”); *see also* Berg, *supra* note 422, at 573.

430. CA 285/73 Lagil Trampolines and Sports Equip. Israel Ltd. v. Nahmias 29(1) PD 63, 75 (1974); CA 764/76 Shimoni v. Ashdod Automobile Factories (M.L.) Ltd., 31(3) PD 113, 115–21 (1977). Scholars have criticized court rulings for being unclear and inconsistent, claiming that the ambiguous and indecisive wording of the Standard Contracts Law further contributed to the problem. *See, e.g.*, Deutch, *Controlling Standard Contracts*, *supra* note 423, at 461.

431. Deutch, *Standard Contracts Act*, *supra* note 423, at 64.

432. *See, e.g.*, *Carnival Cruise Lines, Inc. v. Shute*, 499 U.S. 585 (1991).

Israeli law,⁴³³ such recognition led to legislative amendments enabling the rise of the Israeli purposive approach to unconscionability.

And so, in 1982, the new Standard Contracts Law was enacted, and the Tribunal for Standard Contracts was established.⁴³⁴ The law greatly facilitated the ability of the Tribunal to intervene in standard form contracts. The new law additionally allowed the courts, and particularly the Tribunal for Standard Contracts, a special designated court, to invalidate any unconscionable terms found in standard form contracts, or to decree their amendment.⁴³⁵ Unlike the 1964 law, the application of the 1982 law is broad and encompasses relationships that are not necessarily consumerist in nature.⁴³⁶ Thus, the existence of an unconscionable term is no longer conditional on a monopolistic relationship between supplier and customer.⁴³⁷ The classic literalist approach has been cast aside in favor of a purposive approach. This is only one aspect of a philosophical change that has affected the entire Israeli legal system.⁴³⁸

433. Deutch, *Controlling Standard Contracts*, *supra* note 423, at 475–76.

434. The Standard Contracts Law, 5743-1982, § 37 LSI 6. The Tribunal, a successor of the Board, was granted extensive authority. *See supra* note 425; Deutch, *Controlling Standard Contracts*, *supra* note 423, at 475.

435. The Israeli unconscionability doctrine is incorporated under section 3 of the 1982 Standard Contracts Law. The Standard Contracts Law, 5743-1982, § 3 LSI 6 (“A Court and the Tribunal shall—according to the provisions of this Law—annul or modify any condition of a standard form contract which—having taken into account the conditions of the contract as a whole as well as other circumstances—is oppressive to clients or grants the supplier an unfair advantage, which is likely to result in clients’ oppression.”).

436. *See* CA 294/91 Jerusalem Chevra Kadisha v. Kestenbaum, 46(2) PD 464 (1992).

437. *Id.* The definitions used by the new Standard Contracts Law specifically avoid using the term “consumer,” and instead substitutes the word “client” (or “customer”). The formalistic requirement conditioning the law’s applicability upon the “supply” of a service or product was omitted, and the definitions used for the terms “supplier” and “client” were broadened. The client is defined under section 2 as “a person to whom a supplier proposes that an engagement between them be in accordance with a standard form contract, irrespective of whether he is the recipient or provider of anything.” Thus, the “supplier” may very well be the *recipient* of the product or service with which the contract is concerned. As previously illustrated, this is the case of the adherent-creator type of contract, whereby the drafter is the recipient of the service or product, when the service or product is the adherent’s IP rights (such as ownership, derivative rights, or economic rights). This situation could also occur in the adherent-user type of contract, where the adherent’ rights of fair use are often restricted or waived.

438. *See* AHARON BARAK, *PURPOSIVE INTERPRETATION IN LAW* (Sari Bashi trans., 2007) [hereinafter BARAK, *PURPOSIVE INTERPRETATION*]; *see also* Gabriela Shalev, *Forty Years of Contract Law*, 24 ISR. L. REV. 657 (1990) (explaining how the good faith doctrine was broadened to focus on notions of trust, honesty and fairness, and was applied “widely and generously” by courts).

The general test used in Israel for unconscionability is the “fairness and reasonability” test. Pursuant to this test, a term is considered unconscionable if it seeks to protect the interests or values of one of the contractual parties (namely, the “supplier”) beyond what is perceived as fair in this type of agreement.⁴³⁹ The cornerstone of this approach was laid in the Court’s ruling on the *Kadisha* case, where Barak described the unconscionability test as follows:

What is “unconscionability”? It is a very vague term indeed. . . . It refers to “an unfair advantage obtained through the dictation of conditions.” . . . [W]hen employing the term “unconscionability,” as expressed by the legislature, the court is tasked with introducing social value into what seems to be a form of improper conduct in Israeli society at a given time. The court must determine—based on its understanding of the nature of the contract between the parties on the one hand, and the nature of Israeli social values on the other, whether the contract is fair, or whether it overprotects the supplier’s interests. This process of examination is twofold. First, the relationship between the parties and their typical interests is examined. At the same time, the court considers the social perception of our system with respect to what is regarded as fair and reasonable in a particular type of relationship.⁴⁴⁰

In Israeli law, unconscionability is a standard, an instance of a “valve concept” (*Ventilbegriffe, concetti volvola*),⁴⁴¹ the contents of which change with time and according to circumstances and ever-evolving worldviews and are determined by the interpreter, whose opinion is based on the fundamental principles of the system.⁴⁴² This is a flexible judicial norm that can be adjusted to meet the needs of the time and the place, and is shaped by the courts.⁴⁴³ It draws to

439. CA 1185/97 Milgrom v. Mishan Ctr. 52(4) PD 145 (1998). The principles of the fairness and reasonability test were first introduced in the monumental case of CSC 1/79 Keshet Dry Cleaning Factories Ltd. v. Attorney Gen. 34(3) PD 365, 375 (1980).

440. CA 294/91 Jerusalem Chevra Kadisha v. Kestenbaum, 46(2) PD 464, 529 (1992).

441. AHARON BARAK, HUMAN DIGNITY: THE CONSTITUTIONAL VALUE AND THE CONSTITUTIONAL RIGHT 74 (2015).

442. See, e.g., Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 560 (1992) (“[T]he only distinction between rules and standards is the extent to which efforts to give content to the law are undertaken before or after individuals act.”). Intellectual property regimes often do exhibit unforeseen circumstances in which “[d]etermining the appropriate content of the law for all such contingencies would be expensive, and most of the expense would be wasted.” *Id.* at 622–23.

443. *Id.* at 75; cf. AHARON BARAK, THE JUDGE IN A DEMOCRACY 71 (2006) [hereinafter BARAK, THE JUDGE IN A DEMOCRACY]; BARAK, PURPOSIVE INTERPRETATION, *supra* note 438, at 199. In Deutch’s words, in the context of consumer protection policies (originally, in Hebrew):

some extent from the moral conception of contracts rooted in Hebrew law.⁴⁴⁴

This test confers a great deal of discretion which, at times, involves financial considerations but is primarily driven by moral and social considerations—especially because we are dealing with financial relationships.⁴⁴⁵ This forces us to attribute meanings to a wide variety of rather recondite terms, such as “particular type of relationship,” “the nature of the contract between the parties,” and “the overarching perception of the contract as a whole.”⁴⁴⁶ Such meanings are ever-changing and ever-evolving, and are constantly affected by what is perceived as proper conduct at any given time.⁴⁴⁷ Put simply, an unconscionable condition under Israeli law bespeaks an improper norm.

According to this purposive-interpretative approach, the Israeli doctrine of unconscionability often focuses not only on the nature of the relationship in question, but primarily on the purposes of the laws that pertain to the reviewed contract, as well as the purposes such laws seek to facilitate, beyond the mere interests of the contractual parties.

This was the case in several cases that addressed contracts in the field of banking,⁴⁴⁸ insurance,⁴⁴⁹ contract work, the sale of apartments,⁴⁵⁰ and

Similar to other ‘basket’ provisions or valve concepts [Ventilbegriffe], the unconscionability test incorporated under the Standard Contracts Law is a ‘fluid’ test, which requires the court to take into account broad policy considerations, and a wide system of balances. Therefore, upon determining the application of this concept, one is required to address the fundamental policies underlying consumer laws, within the framework of revealing the appropriate balance between the relevant policies pertaining to the matter.

ORNA DEUTCH, *THE LEGAL STATUS OF CONSUMERS* 458 (2002).

444. CSC 1/79 Keshet Dry Cleaning Factories Ltd. v. The Attorney General 34(3) PD 365 (1980).

445. *Id.* at 373.

446. The unconscionability analysis applies to the content of the term itself, but also considers the “entire contract terms and all the other circumstances.” These “other circumstances” include, inter alia, the nature of the contract, the scope of the contract’s use, and the special characteristics that signify the relationship between the contractual parties. *Id.* at 375.

447. CA 294/91 Jerusalem Chevra Kadisha v. Kestenbaum, 46(2) PD 464, 528–29 (1992).

448. CA 6916/04 Bank Leumi Le-Isr. Ltd. v. Attorney Gen. (Feb. 18, 2010); *see also* CA 232/10 The First Int’l Bank of Isr. v. the Israeli Supervisor of Banks, para. 28 (2012).

449. CA 11081/02 Dolev Ins. Co. Ltd. v. Sigalit Kadosh, 62(2) PD 573 (2007).

450. CA 1632/98 Arbus v. Abraham Rubinstein & Co.—A Contracting Co. Ltd. 55(3) PD 913, 922 (2001); *see also* A ruling by the Tribunal for Standard Contracts (Standard Contracts), SC (Standard Form Contracts) 702/06 Attorney Gen. v. Hous. and Dev. for Isr. Ltd., para. 9 (2011).

employment.⁴⁵¹

This was also the case when the court examined a standard form contract that was drafted by a government institution and sought to establish ordinary pecuniary rights on the one hand, and to facilitate public policies on the other.⁴⁵² Accordingly, this was also the case in which the court reviewed an IP boilerplate.

In the one unambiguous case involving an allegedly unconscionable term in an IP boilerplate, the court acknowledged that the term in question was indeed unconscionable, and that its sole consideration stemmed from the relevant policies that copyright laws seek to facilitate.

In this case, *Jobmaster*,⁴⁵³ the plaintiff sought to restrict users' rights through the terms of use published on its website. These terms constituted a standard form contract under which it was forbidden to copy the want ads published on the website's platform.⁴⁵⁴ Under the ToS, the user "undertakes to make use of the information made available on the website strictly for personal purposes, and to avoid publishing said information or making any commercial use thereof."⁴⁵⁵ Alljobs, the defendant, argued that the want ads consist of a compilation of facts and data, which are not protected by copyright laws. Alljobs argued that it was therefore "allowed to make use of the [data] as it

451. CA 1795/93 Egged Members Pension Fund Ltd. v. Jacob 51(5) PD 433, 451 (1997); see DMS (Regional TA) 8693-09 White Snow (1986) Ltd. v. Eliyahu, p. 3–5 (2011); KG (Regional BS) 3217/09 White Snow (1986) Ltd. v. Lorbrt (2014).

452. SC (Standard Form Contracts) 2016-01 Granot Agric. Coop. Soc'y Ltd. v. Isr. Land Admin., para. 35–45 (2010).

453. HF (Central District) 11359-03-09 Job Master Ltd. v. All You Need Ltd. (2010). The case concerned two claims filed by Jobmaster and the Drushim websites against Alljobs, a company that managed a database of job offers. Alljobs "compiles want ads published in various sources and publishes them on the website it operates." *Id.* at 3 (translated from Hebrew). One of these sources is Jobmaster. Jobmaster alleged, among other things, that Alljobs, in copying its want ads, violated the terms of use published on the website. On these grounds, Jobmaster made several demands, including that the terms of the agreement be enforced against Alljobs, and that Alljobs be prevented from copying these ads. *Id.* at 4.

454. *Id.* at 8–9. When accessing the website, the user is required to confirm that he has read, and has agreed to, the website's ToU. It is not possible, without providing confirmation, to continue accessing the website or to view the ads in question. Section 15 of the terms stated that: "The information published on this website is [Jobmaster's] sole property and [Jobmaster] owns the full extent of the proprietary rights thereto." *Id.* at 11 (translated from Hebrew).

455. *Id.* at 4. Substantively, this is a provision that is similar in essence to the provision considered in the *ProCD* case, where a term restricted the publication and copying of telephone records, information which is not protected under copyright laws in the post-*Feist* era and should be left in the public domain.

deems fit,”⁴⁵⁶ and that Jobmaster could not, by means of a contractual arrangement, namely, the terms of use in its standard form agreement, “create a right out of nothing.”⁴⁵⁷ The court found that a “provision in the agreement which limits the right of the defendant to make use of the data included in the ads is a restrictive provision in a standard form contract and is therefore invalid.”⁴⁵⁸ In other words, the court found this provision to be unconscionable—and did so strictly based on the purposes of copyright laws:

In view of the provisions of the Copyright Law and the above cited case law, it is clear that the information included in these ads is not protected under copyright laws, and it is even expressly excluded from them Copyright law provides protection to a creative work only when such protection serves the interests of society as a whole A restriction on the legitimate use of information that belongs to the public, by means of an agreement which is, in fact, a standard form contract, cannot be permitted.⁴⁵⁹

To clarify, I do not argue that the particular outcome of *Jobmaster*, under which a term that restricts harvesting information is invalid simply because copyright laws do not protect this type of information, is *prima facie* a justified one. Neither is it argued that the purposes of relevant IP laws are the only considerations that must be taken into account when applying the unconscionability doctrine, as they were in the *Jobmaster* case. The goal is to demonstrate that the court, when it examined an unconscionable provision in an IP boilerplate, used the unconscionability analysis, while at the same time considering the purposes of IP laws.

This clearly differs from the application of the doctrine of unconscionability in U.S. case law which focuses, to date, almost exclusively on the consumer-contractual analysis, even when considering a term that pertains strictly to IP rights. Furthermore, in this context, the Israeli court was not at all troubled by the fact that the defendant, Alljobs, is not an ordinary consumer, but rather a sophisticated corporation that provides services that compete with Jobmaster’s, and that Alljobs’ lawyers were entirely familiar with the terms of use and their significance.⁴⁶⁰ Neither was the court troubled by

456. *Id.* at 11–12 (citing TA (TA District) 1074-05 Ma’ariv Modi’in Publ’g Ltd. v. All You Need Ltd. (July 11, 2010); OCR (TA District) 2018/05 Ma’ariv Modi’in Publ’g Ltd. v. All You Need Ltd. (Mar. 3, 2005)) (holding specifically that the content of want ads is not protected by copyright).

457. *Id.*

458. *Id.*

459. *Id.*

460. As previously mentioned, U.S. courts, when applying the unconscionability doctrine to IP boilerplate, have on more than one occasion been interested specifically in the adherent’s level of sophistication, her understanding of the language, whether the adherent is a person or

the fact that Alljobs and other users do not pay for the use they make of the information compiled by Jobmaster.⁴⁶¹ On the contrary, the first words that appear in the court's decision concerning this matter, in the paragraph dedicated to the unconscionability analysis, are "In view of . . . Copyright Law."⁴⁶²

It therefore follows that the purposive approach adopted in Israeli case law enables us—and even obligates us—to consider the purposes of IP laws that pertain to the contractual term under unconscionability. Moreover, this obligation originates from the Israeli standard form contract law, not IP law. Although these are not the *only* purposes that must be taken into account, these are the ones whose consideration we cannot, and must not, avoid.

2. *Unconscionability 2.0: The Advantages of the Purposive Approach*

The fact that Unconscionability 2.0 originates in the Israeli unconscionability doctrine, one that is perceived as a "valve concept" (*Ventilbegriff*), not only accommodates IP policies within its framework, but also confers other advantages that are especially suited to its application to IP boilerplate. Moreover, this doctrine enables us to address problems created by the contemporary adherent-creator type of contract. This Section presents a brief outline of these advantages. As is the case in any theoretical discussion, a practical example will undoubtedly prove beneficial. I will employ the example of the student-creator to this end.

One of the difficulties that previously arose is that IP boilerplate often governs relationships that are not pure-consumerist in nature. This trend, as previously noted, is expected only to increase, and in this context, U.S.

a corporation, whether or not she is engaged in the same business as the offeror, and even whether or not she is receiving the service for free. *See, e.g.,* Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1179 (E.D. Mo. 2004) *aff'd*, 422 F.3d 630 (8th Cir. 2005); Song Fi, Inc. v. Google Inc., No. 14-1283 (RMC), 2014 U.S. Dist. LEXIS 153436 (D.D.C. Oct. 29, 2014); *see also* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 462–63 (2006) ("The law has paid some attention to the impact of terms of use on consumers: virtually all of the courts that have refused to enforce a browsewrap license have done so to protect consumers. Conversely, virtually all the courts that have enforced browsewrap licenses have done so against a commercial entity, generally one that competes with the drafter of the license . . . courts presume that businesses know what they are doing when they access another company's Web site and are therefore more likely to bind them to that site's terms of use. Sophisticated economic entities are unlikely to persuade a court that a term is unconscionable.").

461. *See* Song Fi, Inc. v. Google Inc., 72 F. Supp. 3d 53, 64 (D.D.C. 2014) (holding that "[h]aving taken advantage of YouTube's free services, Plaintiffs cannot complain that the terms allowing them to do so are unenforceable").

462. Of course, this outcome is made possible in part by the fact that Israeli courts, naturally, are not required to tackle issues that pertain to the relationship between federal and state laws that stem from the doctrine of preemption.

unconscionability failed to provide adequate solutions.⁴⁶³ However, the proposed Unconscionability 2.0 enables us to accommodate a broad variety of relationships, including extra-consumer relationships, or, at the very least, relationships that are not consumer-oriented in the classical sense, such as those formed between employers and employees, students and academic institutions, creators and YouTube, etc.

To illustrate this argument, Unconscionability 2.0 could be applied to the IP policies of art and design institutions, which seek to appropriate the IP rights of students. Israeli courts have on more than one occasion analyzed the practices and policies promulgated by academic institutions as standard form contracts.⁴⁶⁴ Although courts have done so in other contexts that do not concern IP rights, it is clear that the main arguments for judicial intervention in standard form contracts apply to such relationships between students and academic institutions, as well.⁴⁶⁵

Another key problem of IP boilerplate was that scholars consistently focused on one or another type of contract. Consequently, no literature could be found that suggests comprehensive solutions to the problem of the IP boilerplate in general. In contrast, Unconscionability 2.0 allows us to address this issue. First, the proposed interpretation does not assume a “one-size-fits-all” approach.⁴⁶⁶ On the contrary, it recognizes the fact that, as explained in Part II, at present IP boilerplate seeks to govern more IP-related issues than ever before, and as such contracts proliferate, they will do so even more. Because each of the many varieties of IP boilerplate merits a different

463. One of the reasons for this is that even though, theoretically, the courts have applied the doctrine to non-consumer relationships—such as contracts governing the transfer of IP rights between an employee and his employer—they have continued to consider the doctrine as though the relationship in question is *essentially* a consumerist one. *See, e.g., supra* note 354.

464. *See, e.g.,* TA (Jerusalem District) 109/94 Isr. Student Ass’n v. Hebrew Univ. of Jerusalem (June 3, 1996).

465. None dispute that there exists a certain dependency between the student and the academic institution. Institutions continuously provide a vital service. They do not function as absolute monopolies, but it most certainly cannot be argued that students enjoy a great deal of bargaining power in choosing their particular academic institution. The student cannot negotiate the provisions in agreements that assign pre-invention (or pre-creation) rights. *See, e.g., Bezalel’s Policy, supra* note 9. Additionally, the academic institute enjoys a superior position in this regard. While the academic institute employs an army of IP lawyers, an ordinary student is unable to understand the legal significance of the terms and conditions imposed on her. She could not reasonably assess the financial consequences of waiving her IP rights, both because she is unaware of her rights to begin with, and because the relevant creation or invention has not yet been created.

466. *See* Abraham Bell & Gideon Parchomovsky, *Reinventing Copyright and Patent*, 113 MICH. L. REV. 231 (2014) (providing a discussion on assumptions such as these in the context of IP law).

approach, the proposed solution is both purposive and broad—it enables us to consider the contract not only as one that regulates IP rights in general, but also according to the particular rights in question.

For example, Unconscionability 2.0 allows us to differentiate between the adherent-creator type of contract and the adherent-user type of contract. It also enables us, under Israeli law, to address the fact that the “supplier” (or offeror) in question is not necessarily an “ordinary” supplier, but may be a hybrid entity or governmental body, as are the academic design institutions.⁴⁶⁷ In this context, Unconscionability 2.0 also incorporates constitutional considerations, in that any provision that restricts the rights of the adherent in terms of her IP is to be regarded with particular suspicion.⁴⁶⁸

The proposed Unconscionability 2.0 does not seek to replace legislative solutions. Quite the contrary: it is intended to solve, among others, the problems produced by private ordering in IP in the absence of relevant legislation, and provides a solution that can be utilized until a time that more suitable regulation is established to redress the matter. This solution would allow the average student to claim ownership over her IP rights in court, notwithstanding the IP boilerplate that assigned her rights, until the legislature restores that students’ ownership by rule of law. The proposed solution enables courts to provide a purposive answer for burning problems that is based on the proper balance dictated by IP policies.⁴⁶⁹ It is able to do so because it is rooted in the Israeli interpretation of the doctrine, because it is a “valve concept” (*Ventilbegriffe*), because it is dynamic, and because it is based on a broad doctrine of unconscionability that enables the introduction of judicial legislation.⁴⁷⁰ Moreover, if unsolvable problems are found—as it is

467. See CA 294/91 Jerusalem Chevra Kadisha v. Kestenbaum, 46(2) PD 464, 492 (1992). When a hybrid entity of this sort enters into a standard form contract, the circumstances mandate a higher standard of fairness compared to private suppliers. This is actually the disturbing case of students being taken advantage of by institutions that are functioning as hybrid entities.

468. *Id.* at 531. In Israeli law, IP has been recognized as a constitutional right pursuant to the Basic Law: Human Dignity and Liberty, 1992-5752 § 3, 45 LSI 150. See CA 2687/92 Geva v. Walt Disney, 48(1) PD 251, 266 (1993); CA 563/11 Adidas Salomon A.G. v. Yassin at 10 (2012).

469. As technology rapidly evolves, this balance changes all the time. See Miriam Bitton, *Modernizing Copyright Law*, 20 TEX. INTELL. PROP. L.J. 65, 72 (2011) (“With the advent of digital technologies, the balances struck by copyright law are also changing.”).

470. See CA 294/91 Jerusalem Chevra Kadisha v. Kestenbaum, 46(2) PD 464, 492 (1992); see also Aharon Barak, *On Society, Law, and Judging*, 47 TULSA L. REV. 297, 299 (2011) (“The judge does not merely declare what the existing law is; he creates new law. In such cases, the judge engages—incidentally to deciding the case—in judicial lawmaking. Such lawmaking . . . creates a general legal norm (ergo omnes) [sic], whether through the force of the principle of stare decisis, or other recognized [techniques] that obligates not only the parties to the dispute,

impossible to provide a regulatory solution to every imaginable unconscionable situation—Unconscionability 2.0 can serve as a complementary solution. Indeed, contract law experts have pointed this out on more than one occasion:

When an abuse is well-defined and identified with a particular economic activity, the remedy may require an invasion of freedom of contract. . . . By contrast, when an abuse is not confined to any one particular activity and cannot be defined except in such general terms as overreaching or unconscionability, the judicial sanction of unenforceability is a more fitting solution. This technique has been legislatively adopted in that section of the Uniform Commercial Code which authorizes courts to refuse enforcement of “unconscionable” clauses in contracts of sale.⁴⁷¹

These insights are particularly useful in the IP setting, when we are often challenged by new versions of IP boilerplate in the aftermath of technological advancements or new innovations.⁴⁷² The most notable advantage of a valve concept is the fact that it “accommodates cases where a flexible legislative arrangement is required, which can be adapted to the needs of the time and place, and hence allows us to avoid a strictness that could potentially lead to arbitrariness.”⁴⁷³ IP boilerplate takes many forms, they constantly evolve, and they regularly present us with additional challenges that are brought about by the advent of new technologies. This naturally prevents us from predicting the nature of obstacles yet to come.

Indeed, some may argue that the use of valve concepts serves only to spread uncertainty in the world of law.⁴⁷⁴ It is true that the proposed solution is flexible by nature, and even, some might say, unpredictable. But it is this flexibility that makes it so potent, allowing it to uphold the proper balance

but all branches of the government and members of the public.”); cf. BARAK, *THE JUDGE IN A DEMOCRACY*, *supra* note 443, at 71.

471. Alfred W. Meyer, *Contracts of Adhesion and the Doctrine of Fundamental Breach*, 50 VA. L. REV. 1178, 1186 (1964).

472. For example, Instagram, the popular content-sharing platform, included, for a certain period, a provision under its terms of use that enabled it (and even *other* third parties) to distribute and publish content uploaded by users for *commercial purposes*, without any compensation guaranteed to the user. See Kurt Opsahl, *Instagram’s New Terms of Service to Sell Your Photos*, ELEC. FRONTIER FOUND. (Dec. 18, 2012), www.eff.org/deeplinks/2012/12/instagrams-new-terms-service-sell-your-photos [https://perma.cc/GC7V-42F7].

473. VARDA LUSTHAUS & TANA SPANIC, *STANDARD CONTRACTS* 37 (1994) (translated from Hebrew).

474. *Id.* at 38; see also BARAK, *THE JUDGE IN A DEMOCRACY*, *supra* note 443, at 71 (“The decision to resort to a vague concept . . . means taking the risk, *ex ante* that uncertainty will result from the need to assign weight to clashing values. Moreover, he who desires to refrain from granting discretion to judges should not resort to vague concepts . . .”).

between the various purposes of IP laws.

In previous Parts, I demonstrated how some inter-doctrinal solutions suffered from a utilitarian bias. Unconscionability 2.0 allows us to address this on a number of levels. First, according to the purposive approach, courts analyzing unconscionability must be guided by a “moral or social consideration.”⁴⁷⁵ Furthermore, as a “balance-based”⁴⁷⁶ approach, Unconscionability 2.0 facilitates the accommodation of a wide variety of competing considerations. A narrow analysis of a particular unconscionable provision could potentially lead to judicial challenges. To illustrate, consider the adherent-creator contract that governs students’ creations. The IP policy of Seminar Hakibbutzim, an Israeli academic institution, stipulates:

Copyrights, as well as any other intellectual property rights, to any work, and to the imprint or the fixation of any [work based on] such intellectual property rights (hereafter a “Creation”) created by students in the course of or pursuant to their academic education, or in the course of utilizing the College’s resources, including the ownership over any object in which the original Creation is fixed or incorporated, constitutes the sole property of the College throughout the period of [duration of the] rights, and anywhere in the world.⁴⁷⁷

Such a provision, or any provision, that seeks to transfer ownership over an invention or a creation from the student to an academic institution serves as a pathological example of an unconscionable provision. It does not seem to support the purposes of IP law. Indeed, it actually fails to give students the proper incentive to engage in creative art. On the contrary, such a provision actively discourages creative undertakings. Consider, for example, the case of a student who has never bothered to read the institution’s policy, and who creates an invention or an original work of art—only to learn later that this invention or work of art now fully belongs to the institution, and that she is strictly forbidden from using or publishing it.⁴⁷⁸ Such a student might find herself so utterly frustrated by the arbitrariness of this state of affairs that she might decide to discontinue any creative-inventive efforts not only during her

475. *Kadisha*, *supra* note 436, at 529 (translated from Hebrew).

476. See, e.g., Gideon Parchomovsky & Kevin A. Goldman, *Fair Use Harbors*, 93 VA. L. REV. 1483, 1491–94 (2007); Lior Zemer, *The Conceptual Game in Copyright*, 28 HASTINGS COMM. & ENT. L.J. 409 (2006); Lior Zemer, *Authors and Users: Lessons from Outre-Mer*, 25 INTELL. PROP. J. 231 (2013).

477. Seminar Hakibbutzim, *Students Regulations for the Academic Year of 5775 (2014–2015)—Annex 7 Copyrights* 56 (2014), www.smkb.ac.il/filehandler.ashx?fileid=546887 [hereinafter *Seminar Hakibbutzim’s Policy*] (translated from Hebrew).

478. Such a restriction is also included under *Bezalel’s Policy*, *supra* note 9, at §§ 1, 4.

academic career, but later in her life, as well. However, is it reasonable to consider this limiting provision only from the vantage point of the utilitarian approach?⁴⁷⁹

The utilitarian approach primarily focuses on society as a whole, rather than the individual. It concerns itself, then, with the total sum of utilities—the individual, and even the law, are instrumental to this equation, which seeks to facilitate the cumulative utility of all members of society.⁴⁸⁰ It can therefore be described as an arithmetic model:⁴⁸¹ if we subtract “pain” and add “pleasure,” we will eventually arrive at the cumulative happiness of individuals, which is expressed by “maximum utility.”⁴⁸² Given the many advantages of encouraging individuals to produce original creations and inventions, it behooves the law to acknowledge IP rights to the extent necessary to maximize the public interest, and, necessarily, to do so irrespective of the considerations relating to individual creators and inventors.⁴⁸³

479. Expressions of the utilitarian approach can be found in a wide variety of historical sources, and it is primarily associated with Anglo-American traditions. Notable among the sources found in literature is the Statute of Anne, which granted authors the right to publish and copy books, thus for the first time acknowledging authors as the legal owners of the IP rights to their work. Another prominent source is, of course, the U.S. Constitution (U.S. CONST. art. I, § 8, cl. 8); cf. Justin Hughes, *The Philosophy of Intellectual Property*, 77 GEO. L.J. 287, 303 (1988). The U.S. Supreme Court has emphasized in a number of significant opinions the “substantive” and “true” purpose of IP laws, in the spirit of the U.S. Constitution. See also *Feist Publ’ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 349–50 (1991) (“The primary objective of copyright is not to reward the labor of authors, but ‘to promote the Progress of Science and useful Arts’ To this end, copyright assures authors the right to their original expression, but encourages others to build freely upon the ideas and information conveyed by a work.”); *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975) (“The immediate effect of our copyright law is to secure a fair return for an ‘author’s’ creative labor. But the ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good.”); *Harper & Row Publishers v. Nation Enters.*, 471 U.S. 539, 558 (1985).

480. JEREMY BENTHAM, AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION xlvii (1879) (“The consequences of any Law, or of any act which is made the object of a Law, the only consequences that men are at all interested in, what are they but *pain* and *pleasure*.”).

481. Bentham asserts that the law is a simple mathematical calculation whose result is certain, and that, even though concerned with morality, the law is no different from any other mathematical calculation. JEREMY BENTHAM, PRINCIPLES OF LEGISLATION 32 (1830) (“These are the elements of moral calculation; and legislation thus becomes a matter of arithmetic. The *evil* produced is the outgo, the *good* which results is the income.”).

482. Richard A. Posner, *Utilitarianism, Economics, and Legal Theory*, 8 J. LEGAL STUD. 103, 111 (1979). And what about happiness? Happy individuals are those who can achieve their wishes according to a hierarchy of preferences that maximizes their utility. *Id.*

483. ROBERT P. MERGES, JUSTIFYING INTELLECTUAL PROPERTY 2–3 (2011).

Against the creator's social contributions to the welfare and prosperity of society through its creation of intellectual goods, one weighs the social loss reflected in monopolies, namely, the loss suffered by consumers owing to the fact that the goods in question are sold at a price that exceeds the marginal cost entailed in their production.⁴⁸⁴ Therefore, IP laws are designed so as to create a formula that produces an optimum (in terms of quality and quantity) of intellectual goods.⁴⁸⁵

The economic approach subsequently replaced the term "utility" with social "welfare,"⁴⁸⁶ but whether we are engaged in maximizing utility or in maximizing cumulative welfare, both of these approaches are concerned with society rather than the individual, with the facilitation of public interests as opposed to an outcome that promotes particular justice.⁴⁸⁷ An exhaustive discussion of these approaches lays beyond the scope of this Article, but the main point here is that these approaches will always consider the individual as a tool who is to be rewarded in order to provide her with an incentive to enrich our world with her products and creations—all in the name of progress, expression, and diversity.⁴⁸⁸ These approaches assume that, in the absence of reward, and in the absence of property protection, the individual would simply

484. *Id.*

485. *Id.* This pretense, some may argue, of the utilitarian approach is one of the most notable objections raised by its critics. Can we really assess the social contribution of works of art and inventions using estimates? Is there such a thing as "an optimal quantity of social goods?" Merges asserts that "we will never identify the 'optimal number' of patented, copyrighted, and trademarked works." *Id.* at 3.

486. Posner, *supra* note 482.

487. Palmer argues that despite the methodological distinction proposed by Posner in his scholarship, the economic approach to IP still draws on Benthamite discourse, and that despite the use of the term "welfare" rather than "utility," its normative roots have remained the same. See Tom G. Palmer, *Intellectual Property: A Non-Posnerian Law and Economics Approach*, 12 *HAMLIN L. REV.* 261, 262 (1988). Yet, the interest of society in general could be aligned with moral or social driven consequences. See generally Oren Bracha & Talha Syed, *Beyond Efficiency: Consequence-Sensitive Theories of Copyright*, 29 *BERKELEY TECH. L.J.* 229 (2014) (reconciling consequence-sensitive theories of copyright with moral theories).

488. At the backdrop of the utilitarian and non-utilitarian "skirmishes" that are taking place in IP scholarship in the last decades (and have recently somewhat reached a peak, see *supra* note 492 for a discussion), some scholars tried to ease the debate by suggesting that empirical evidence proves that treating creators morally maximizes the social welfare. Stephanie Plamondon Bair, *Rational Faith: The Utility of Fairness in Copyright*, 97 *B.U. L. REV.* 1487, 1531 (2017) ("[T]reating creators fairly results in real efficiency gains by motivating creative behaviors, enhancing the quality of creative output, and bringing copyright policy in line with the moral intuitions of legal decision makers and the general public."). These findings and arguments help us reach a consensus on the operation of midlevel principles, but do not solve the fundamental problem of what should be done in other cases where social welfare would be maximized by *not* adhering to deontological principles. See Merges, *Against Utilitarian Fundamentalism*, *supra* note 53.

avoid creating. Or, at the very least, her creations would be of poorer quality,⁴⁸⁹ and in this respect creative activity is regarded as a demanding or even “unpleasant”⁴⁹⁰ pursuit. These approaches assume that efficient allocation means that society benefits as a whole, even if the individual suffers or endures injustice: that is to say, even if he is oppressed and mistreated.⁴⁹¹ Therefore, the proposed solution does not allow us to address purely utilitarian considerations, as it is based on a moral foundation and fosters conceptual pluralism.

In that sense, the proposed solution tries to shatter the utilitarian hegemony as well,⁴⁹² at least when it comes to the discussion of IP boilerplate.

489. MERGES, *supra* note 483, at 2 (“Society offers above-market rewards to creators of certain works that would not be created, or not created as soon or as well, in the absence of reward.”); *see also* Mark A. Lemley, *Property, Intellectual Property, and Free Riding*, 83 TEX. L. REV. 1031 (2005).

490. Hughes, *supra* note 479, at 304 (“The wide acceptance of the instrumental argument suggests wide acceptance of the premise that idea-making is a sufficiently unpleasant activity to count as labor that requires the inducement of reward.”).

491. This principle affords a great amount of flexibility to the utilitarian approach in shaping the rights of individuals. It is also one of the foremost critiques of the moral aspect of the utilitarian approach, in view of its indifference to means that have maximized happiness (in this context, the “sadism example” merits our attention in particular. On the other hand, according to the financial approach to IP, we could argue that this state of affairs is not Pareto preferable, and certainly not Pareto efficient. Even though society benefits, and the happiness of others can be improved, at least one individual would suffer as a result of the allocation of rights). *See* Andreas Rahmatian, *A fundamental critique of the law-and-economics analysis of intellectual property rights*, in *METHODS AND PERSPECTIVES IN INTELLECTUAL PROPERTY* 71, 77 (Graeme B. Dinwoodie ed., 2013). Clearly, policymaking under this criterion creates difficulties, since it could be argued that the allocation of a certain right to one comes at the expense of the other. *Id.* at 77. Therefore, the economic approach relies primarily on the criterion put forth by Kaldor-Hicks, according to which an effective policy allows the “beneficiaries” to compensate the “injured” for the allocated right, and most importantly, increases the aggregate welfare (through the beneficiaries’ excess revenue). *Id.* at 78.

492. The term “utilitarian hegemony” means that, despite the extensive theoretical body of literature on personality-based theories of copyright, and the views furthered by cultural-modern approaches, the main argument remains that the allocation of rights to IP is designed to serve *society as a whole*, and from this Archimedean view we derive the proper balancing point that demarcates the scope of monopolistic rights. This balancing point ensures that enough remains in the hands of the public so as to reward the authors and creators of the future, while incentivizing the authors and creators of today. This “hegemony” recently manifested in a controversial article by Lemley, suggesting that basically all non-utilitarian approaches which are not grounded on empirical evidence are akin to faith-based beliefs and are therefore irrational. *See* Mark A. Lemley, *Faith-Based Intellectual Property*, 62 UCLA L. REV. 1328 (2015). *But see* Merges, *Against Utilitarian Fundamentalism*, *supra* note 53. The utilitarian approach draws in part on theoretical and philosophical justifications for granting private property protection, in general. The details of the theories that justify private property are beyond the scope of this paper, as are those of the scholarly debate as to whether tangible private property justifications

This advantage allows Unconscionability 2.0 to surmount the transition to the adherent-creator type of contracts, and to adapt itself to the age of user-generated content, in which creations are not produced primarily for money—but for other purposes.⁴⁹³

Therefore, according to the proposed solution, the pathological provision cited above would always be considered from the moral-deontological standpoint as well, which acknowledges the fact that students must be rewarded for their contributions to society.⁴⁹⁴ This perception also allows us to address more ambiguous cases as well, such as that of the provision considered in *Jobmaster*, in which a drafter sought to privatize information that belongs to the public. A moral analysis of this provision would not permit its enforcement. Instead, it would require the offeror to leave these objects as they are.⁴⁹⁵ It would also invalidate a provision in a sharing platform ToU that prevents users, without justification, from deciding the fate of their own creations, in view of the special connection that is formed between creators and their creations—as an integral part of one’s personality.⁴⁹⁶

IP boilerplate tends to deprive original creators of control over their own creations. At times, in difficult cases, a utilitarian analysis would seemingly lead us to conclude that this practice is justified.⁴⁹⁷ The proposed solution forces us to engage in a moral-deontological debate that acknowledges the creator’s

are applicable to IP, and vice versa. *See, e.g.*, PETER DRAHOS, A PHILOSOPHY OF INTELLECTUAL PROPERTY 5 (1996); *cf.* MERGES, *supra* note 483, at 4.

493. *See, e.g.*, YOCHAI BENKLER, *supra* note 84; *see also* WILLIAM PATRY, MORAL PANICS AND THE COPYRIGHT WARS 67–68 (2009) (providing more on the assertion that historically, in general, creators do not engage in creation because of the proprietary protection of copyrights).

494. The roots of the deontological approach can be found in John Locke’s notions known as the “labor theory of property.” Under that approach, the natural right of a person to the fruits of her labor is based on the idea that, just as her body is her own, so are her creations. The invention or creation that one fashions and creates with one’s hands and mind is also one’s property. *See* JOHN LOCKE, TWO TREATISES OF GOVERNMENT, 134–438 (Peter Laslett ed., Cambridge Univ. Press, 2nd ed. 1988) (1689); Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533 (1992); *cf.* MERGES, *supra* note 483, at 32; LIOR ZEMER, THE IDEA OF AUTHORSHIP IN COPYRIGHT (2007).

495. Lior Zemer, *The Making of a New Copyright Lockean*, 29 HARV. J.L. & PUB. POL’Y 891 (2005).

496. According to personality-based theories, the creative work, being as it is an expression of one’s personality, endows the creative author with control over the creation’s fate. Hughes, *supra* note 479, at 330. One finds an instance of this provision in Instagram’s terms of use, which enabled the platform, for a short period, to commercialize the images produced by adherent-creators. *See supra* note 472 (providing more detail about this issue).

497. It could be argued that given the vast knowledge maintained by academic institutions, they could make creations and patents accessible to the public in a more proper fashion.

autonomy in a manner that, as Merges put it, “[allows] individuals to control the works they create.”⁴⁹⁸

But the proposed solution also incorporates other theories. Some recent cases indicate that courts have begun to consider rival theories in deciding IP issues.⁴⁹⁹ The utilitarian approach has begun to give way to personality-focused approaches on the one hand, and culturally-focused approaches on the other. Both approaches acknowledge the significant role of the public domain, not only as the recipient of the creative work, but also as a generator of meaning.⁵⁰⁰ This shift mandates a pluralistic, inclusionary approach to the purposes of IP law, which fosters a theoretical discourse that relies on a broad assortment of theories, and on the existence of a dialogue and interrelationships between policies.⁵⁰¹ The proposed solution allows us to readily incorporate such a pluralistic approach. Being as it is a flexible and balance-based tool, it not only encourages, but requires, a discourse of varying purposes.

Moreover, even without agreeing on the foundational justification for each particular result, be it utilitarian, deontological, or dialogical, Unconscionability 2.0 invites debaters to meet on a “common space” or “place of engagement,”⁵⁰² since it operates on the doctrinal level on which consensus can be found as to the “operational details of the IP system”⁵⁰³ while putting aside foundational disagreements.⁵⁰⁴

IP boilerplate, and in particular the adherent-creator type of contract, present us with issues and difficulties whose solutions mandate a broad, purposive approach. For example, in the case of user-generated content, some claim that because of the personhood and personality-based motivations to engage in these creations that reflect one’s identity, there is a need to evaluate users’ waivers of copyrights in their creations in ToU on a spectrum, “where

498. MERGES, *supra* note 483, at 289.

499. *See, e.g.*, *Bikram’s Yoga Coll. of India, L.P. v. Evolution Yoga, LLC*, 803 F.3d 1032, 1037 (9th Cir. 2015) (citing *NIMMER & NIMMER*, *supra* note 314, at § 19E.04[B]) (“[F]ree access to ideas is vital not only for copyright law but also for the maintenance of the democratic dialogue.”); *see also* *CA 5097/11 Tiran Communications (1986) Ltd. v. Charlton* (2013) (providing an example in Israeli law).

500. *See, e.g.*, CRAIG, *supra* note 92, at 3; Zemer, *Dialogical Transactions*, *supra* note 92; *see also* DRASSINOWER, *supra* note 48; ROSEMARY J. COOMBE, *THE CULTURAL LIFE OF INTELLECTUAL PROPERTIES: AUTHORSHIP, APPROPRIATION, AND THE LAW* (1998); OCR (TA District) 11646/08 *The Football Ass’n Premier League Ltd. v. John Doe* (2009) (providing an Israeli copyright law example).

501. *Cf.* Merges, *Against Utilitarian Fundamentalism*, *supra* note 53.

502. MERGES, *supra* note 483, at 10.

503. Merges, *Against Utilitarian Fundamentalism*, *supra* note 53, at 706.

504. *Id.* In Merges’ terms, argumentation on the application of Unconscionability 2.0 can operate on “levels 1 and 2 without the need for deep agreement, all the way down to level 3.” *Id.*

rights that are more personal are harder to alienate and subject to stricter judicial scrutiny.”⁵⁰⁵ Unconscionability 2.0 can accommodate this type of nuanced analysis.

This can also be demonstrated by the problem of the student-creator. Many policies define the term “College Resources” exceedingly broadly, so as to allow the institution to secure (and appropriate) as many creations as possible. For example, Seminar Hakibbutzim’s policy stipulates that these resources include “all of the resources made available to the students by the College, including instruction and teaching sessions, as well as physical means and resources.”⁵⁰⁶ Therefore, a student who has read the policy, and who wishes to retain her IP rights, will most likely avoid conversing with other students or teachers about her potential ideas for creations or inventions, be it in class or elsewhere at the college. Such provisions are detrimental to IP purposes, not only on utilitarian grounds, but because they inhibit the sort of interpersonal interactions that serve as the breeding ground for intellectual activity.⁵⁰⁷ Furthermore, they prevent the basic dialogue on which human creativity is founded.⁵⁰⁸ Unconscionability 2.0 would void such terms, not only because they fail to provide adequate incentives for creators, but also because they fail to encourage discourse and a healthy exchange of ideas and opinions.⁵⁰⁹

3. *The Adoption of Unconscionability 2.0 in U.S. Law*

The Israeli solution can be implemented in U.S. law. As demonstrated in the previous Section, the doctrine’s inefficacy as a solution to the IP boilerplate problem is chiefly caused by a formalistic consumer-oriented interpretation.⁵¹⁰ The legislative history of the U.S. unconscionability doctrine is extensive; a full account of such history is beyond the scope of this Section. However, a brief

505. Storella, *supra* note 78, at 2048 (explaining that if the personal nature of a work implicates personhood concerns, a stricter scrutiny for users’ waivers is required).

506. *Seminar Hakibbutzim’s Policy*, *supra* note 477, at 56 (translated from Hebrew).

507. Lior Zemer, *Towards a Conception of Authorial Knowledge in Copyright*, 3 BUFF. INTELL. PROP. L.J. 83, 85 (2006) (“Manifestations of authorial knowledge, however, are socially and culturally constructed. They are not created from thin air and are products of social interaction and collective cultural collaborations.”).

508. *See* Zemer, *Dialogical Transactions*, *supra* note 92; *cf.* DRASSINOWER, *supra* note 48 (suggesting a communicative account to copyright).

509. *Cf.* Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L.J. 283 (1996) (proposing a democratic paradigm to copyright).

510. *See also* Richard L. Barnes, *Rediscovering Subjectivity in Contracts: Adhesion and Unconscionability*, 66 LA. L. REV. 123, 152 (2005) (stating that, in the contractual context, “[c]ourts emphasize the flexibility of the concept, but remain centered on the concepts of unfairness in the bargaining process and unfairness in the result reached by the bargaining parties”).

review discloses no fundamental principles that would appear to prevent the implementation of the proposed solution by U.S. courts. And as mentioned, the Restatement also accommodates a broader application of unconscionability.

As Leff has noted in his monumental article on the doctrine, the intentions and concerns of the drafters of the U.C.C. unconscionability doctrine were not solely affected by issues of power inequality, bargaining power, and “the opportunity to read.” The situation was quite the contrary: “[n]o doubt the overall drift of the section was that contracts ought to be ‘fair and balanced’ no matter how the parties bargained.”⁵¹¹

The purpose of the U.C.C. section on the unconscionability doctrine, it was argued, was to replace unconscionable terms with more balanced and fair ones—according to the specific needs of the transaction or the trade in question.⁵¹² Therefore, even if the adherent is completely conscious, and the parties have engaged in negotiations (in other words, there has been “considered and deliberate action”),⁵¹³ if the outcome of the contract is unbalanced or unfair according to the needs of the relevant trade, the contract would not be enforced.⁵¹⁴ Under this perception, not only provisions that “shock the conscience” would be subject to invalidation.⁵¹⁵ Indeed, the Official Comments to the U.C.C. set a high substantive and procedural bar for unconscionability⁵¹⁶ that courts followed. But as the recent Restatement suggests,⁵¹⁷ and as Deutch claimed 40 years ago, such comments should be put in context: “[i]t would be wrong to regard the Official Comments as more than a general explanation only partially covering the scope of the doctrines.”⁵¹⁸ Since then, scholarship has showed, on multiple occasions, that unconscionability could be used to serve its purpose and should be better

511. Leff, *supra* note 237, at 491; *see also id.* at 490 (“[T]here were hints that perhaps there were some contracts or clauses which, under the general rubric of ‘unconscionability,’ would not be enforced regardless of what the bargaining process was like.”).

512. *Id.*

513. *Id.*

514. *Id.*

515. *See supra* note 247; *see also* James R. Maxeiner, *Standard-Terms Contracting in the Global Electronic Age: European Alternatives*, 28 YALE J. INT’L L. 109, 172 (2003) (“If the American system is less ambitious than its European counterparts and is largely limited to striking down terms that ‘shock the conscience,’ it has not been by design. When American legislatures enacted U.C.C. section 2-302, they adopted a provision that its drafters hoped would allow American courts to develop ‘machinery’ for ‘policing’ contract terms.”).

516. *See supra* note 237.

517. Although not explicitly acknowledging that, the Restatement did reformulate the doctrine and effectively lowered the thresholds. *See* Section III(A) “Why Unconscionability?”

518. SINAI DEUTCH, UNFAIR CONTRACTS: THE DOCTRINE OF UNCONSCIONABILITY 55–56 (1977).

aligned with its origins.⁵¹⁹

While it could be claimed that most de facto IP regulation is conducted via boilerplate, and not negotiated contracts or law, we have yet to devise a tool that operates exactly in those realms. In the absence of such a tool, courts have resorted to creative solutions, adapting misuse to address the gap. Meanwhile, scholars have long suggested (and continue to suggest) that we need “copyright and contract [to] work better together, towards a more copyright-contract-centric [regime],” one in which “freedom of contract needs to be in check.”⁵²⁰ But the Restatement brings about a new opportunity to use an existing doctrine to that effect, with a refreshing view that aligns (as much as possible) unconscionability with its normative purpose. Moreover, as Beh explains, the animated debates around unconscionability of arbitration clauses have revived the judicial application of unconscionability in the United States. This awakening, Beh asserts, “reveals that, at least with regard to arbitration, judges have reached a tipping point.”⁵²¹ Knapp also joins this view, suggesting “a possibly wider and more significant role for the concept of unconscionability as the new century unfolds.”⁵²² I propose this role promises a more prominent impact in the realm of IP through Unconscionability 2.0.

4. *Unconscionability 2.0 in Negotiated Contracts and Between Sophisticated Parties*

Under Israeli law, a term that is negotiated for a specific transaction, in a specific contract, and agreed upon by the parties, is explicitly excluded from the application of the law of Standard Form Contracts and the doctrine of unconscionability.⁵²³ The law specifically requires both parties to consent to such excluded term. This definition has not been tested in courts because in cases that involve a term that undermines public policy, courts prefer to use another purposeful and robust mechanism under Israeli contract law: the public policy exception. However, some cases cited both doctrines to void an unconscionable term.⁵²⁴

Ad hoc negotiated contracts can also include terms that undermine and displace IP policies. The best example is the long tradition of misuse cases

519. See Hazel Glenn Beh, *Curing the Infirmities of the Unconscionability Doctrine*, 66 HASTINGS L.J. 1011 (2014).

520. D’Agostino, *supra* note 47, at 29.

521. Beh, *supra* note 519, at 1033.

522. Knapp, *supra* note 260, at 326.

523. The Standard Contracts Law § 2 (1982) (defining “condition” as a “stipulation in a standard form contract . . . but does not include a stipulation specially agreed upon by a supplier and a customer for the purposes of a particular contract”).

524. CA 294/91 Jerusalem Chevre Kadisha v. Kestenbaum, 46(2) PD 464, 538 (1992).

involving sophisticated commercial parties in negotiated licenses.⁵²⁵ Another example is the rights of authors, freelancers, and artists who are often coerced in negotiated contracts, in which the adherent has very little (but some) negotiating power.⁵²⁶

In this context, it is important to draw a clear distinction between a negotiated contract, a boilerplate offered to sophisticated parties who may use the product for commercial and business purposes, and other boilerplate. Sometimes the same boilerplate is offered to users in the market, and the user just happens to be a sophisticated player. That was the case in *Disney*, *Lexmark*, *ProCD*, and the Israeli case, *Jobmaster*. Sometimes the boilerplate is offered on a take-it-or-leave-it manner only to businesses. In both cases, under the Israeli and the proposed Unconscionability 2.0 approaches, there is reason to apply unconscionability. The same approach could be applied in U.S. law: under the Restatement, “[a] finding of procedural unconscionability based solely on the fact that a contract was in standard, non-negotiable form, without more, constitutes the lowest quantum of procedural unconscionability and would have to be matched with a high degree of substantive unconscionability to render the contract or term unenforceable.”⁵²⁷ In this case, the main concern is not the level of parties’ sophistication but rather the salience of the terms and whether they are offered on a take-it-or-leave-it basis.

More importantly, even if the adherent is a so-called sophisticated party, terms could be nonsalient, because there is no market competition over the quality of such terms that could discipline the drafter, because there is no “market” for these specific terms (as opposed to the warranty, price, etc.). In IP, each and every innovation or creation is unique and often so is the market to comment on, use, resell, tinker with, and perform fair use on the work or innovation, as well as the externalities created by over-monopolization of such work.⁵²⁸

It follows that in most cases, IP subject-matter terms are nonsalient ab initio because of the nature of the rights they seek to control. These contracts reflect a situation in which “external circumstances (not created by the business) . . . compelled consumers to execute the contract” and consumers “are compelled to transact with the business regardless of the standard

525. See, e.g., *Gen. Talking Pictures Corp. v. W. Elec. Co.*, 305 U.S. 124 (1938).

526. D’Agostino, *supra* note 47, at 10 (discussing the case of coerced freelancers in creative industries).

527. See The Restatement, *supra* note 29, at 80.

528. See, e.g., *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994); Wendy Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and Its Predecessors*, 82 COLUM. L. REV. 1600 (1982).

contract term.”⁵²⁹ Moreover, if all the drafters in a relevant market (even if we could identify such a market) have “similar pro-business terms,” “that does not negate a finding of procedural unconscionability” as long as the term does not affect the decisions of a large group of consumers.⁵³⁰

This suggests that since the procedural prong of unconscionability is addressed through the consideration of salience, the focus of the inquiry should be the substantive prong in which the level of sophistication of the parties is less of a concern, and there is no reason to neglect consideration of the relevant IP policies at hand. Moreover, under a sliding scale approach, a higher “quantum” of substantive unconscionability could be inferred in cases where public policy considerations are undermined, which is often the case in IP.

Still, there is a catch. The Restatement and the U.C.C. doctrine of unconscionability both follow a different definition of adherent, one that is limited to consumers in their traditional sense: “[a]n individual acting primarily for personal, family, or household purposes.”⁵³¹ Courts would be reluctant to apply unconscionability in cases involving sophisticated parties. In this context I would argue that differentiating between consumers and commercial parties makes little sense from both a contract and IP perspective.

From a contract perspective, as some scholars claim, a standard form contract offered to small businesses could exhibit the same asymmetric disparities of a consumer contract.⁵³² Small businesses cannot simply negotiate a contract just because the product is offered for business use, rather than for household use. Also, consumers are not affected by IP policies in the same manner as are businesses, and it is unrealistic to expect small businesses to “make decisions” based on the quality of these terms in a manner that polices such terms. In any event, in most cases, the boilerplate in question is in fact a “consumer contract” (it is offered also to consumers, even if these consumers are not the litigants in the case brought to the court), and therefore courts should assume terms are nonsalient.

From an IP perspective, this distinction does not bring us closer to disciplining IP boilerplate and preventing its abusive effects. That is perhaps why courts seem to be in need of a more nuanced tool to allow them to refuse to enforce mass-market terms in some cases involving commercial parties (like *Lexmark*), and reach different results in other cases. Because Unconscionability

529. The Restatement, *supra* note 29, at 82.

530. *Id.* at 81.

531. *Id.* at 8, 14; *see also* U.C.C. § 2-104 (AM. LAW INST. & UNIF. LAW COMM’N) (providing the definition used by the U.C.C.).

532. Larry T. Garvin, *Small Business and the False Dichotomies of Contract Law*, 40 WAKE FOREST L. REV. 295, 386 (2005).

2.0 enables the court to consider the servitude-like nature of a term and its salience as part of its application, it serves as that tool, where the traditional doctrine of misuse could be used to police negotiated egregious contracts on a case-by-case basis. Most importantly, Unconscionability 2.0 could be used to refuse enforcement of the contract, and not just as a defense from copyright or patent infringement. The distinction between misuse and Unconscionability 2.0 becomes clearer when considering a more proactive and robust application of unconscionability than is currently available in the United States, one that is proposed in the following Sections.

B. A ROBUST VISION FOR UNCONSCIONABILITY 2.0

1. *Presumptions of Unconscionability 2.0*

One of the key shortcomings of unconscionability and other equitable defenses is that they are costly to litigate, and impose the burden of proof on the adherent (or defendant in the context of misuse).⁵³³ As a litigation-based tool, unconscionability could not serve as a comprehensive solution to this problem, nor will it fully internalize the costs that harmful appropriating contracts impose on society. Scholars have also recognized this specific potential shortcoming of unconscionability in the context of private ordering and IP, noting that relying on a few users to bring suits that will shape policies is, in general, problematic.⁵³⁴

Yet case law, including landmark and strategic litigation, has always been instrumental to the adaptation of IP laws, as technology has developed and new challenges have presented themselves. That has been the case in critical junctions of IP, such as fair use, first-sale, preemption, misuse, and copyrightability of software.⁵³⁵ Sometimes it even involved the “little guy or gal” challenging well-resourced giants, supported by amici from nonprofit organizations and academia.⁵³⁶ In the context of unconscionability, much like fair use, establishing precedent on a case-by-case basis could influence all segments of boilerplate, bringing a sea change to a specific industry and its abusive practices.

Yet there are ways to reformulate unconscionability into a more effective tool by imposing the burden of proof on the drafter, and potentially shifting the cost of litigation as well. According to this principle, adopted under Israeli law, if a term in a standard form contract meets the criteria of unconscionability presumptions, the burden of proof is borne by the drafter,

533. See Pallas Loren, *supra* note 46, at 531; RADIN, *supra* note 1, at 128–30.

534. See Pallas Loren, *supra* note 46, at 520.

535. See, e.g., Menell, *This American Copyright Life*, *supra* note 58; see also Menell, *Rise of the API Copyright Dead?*, *supra* note 116.

536. *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150, 1155 (N.D. Cal. 2008).

who must prove that, in view of the contract as a whole and its particular circumstances, the condition in question is justified and reasonable.

In the United States, a few states have enacted unfair and deceptive practices statutes adopting this principle, setting forth factors that are presumed to be unconscionable.⁵³⁷ The U.C.C. also incorporates presumptions of unconscionability.⁵³⁸ So does the Restatement, to a limited extent.⁵³⁹ Still, these presumptions are used narrowly and in egregious cases.⁵⁴⁰ They serve to codify existing case law, as opposed to setting a policy agenda for what is normatively desired, taking into consideration the litigation costs imposed on consumers. Moreover, the ALI Principles of Software Contracts adopted a limited “gray list” of terms that should be looked at with suspicion as part of the unconscionability analysis, yet as explained, that list is focused more on matters of contractual unfairness, and less on matters of IP abuse.⁵⁴¹

In a contrary manner, Israel has taken a proactive approach to unconscionability, adding multiple presumptions to the law to set a policy agenda of deterrence, setting new limitations on what drafters may do with contract. The new amendment introduced in 2014 to the Standard Form Contracts Law, for example, did not seek to codify or restate existing case law—but rather to expand the list of *prima facie* voidable terms, enabling consumers to swiftly resolve cases.⁵⁴² As such, under Israeli law, among others, arbitration clauses, or other terms that limit the consumer’s available remedies or rights under law are presumed to be unconscionable.⁵⁴³

How can presumptions of Unconscionability 2.0 advance IP policies? Presumably, one potential doctrinal solution would be including a presumption whereby a term in an IP boilerplate that limits, restricts, or conditions a right (or privilege) assigned to the user or the creator under IP laws (a statutory right), is presumed to be unconscionable—shifting the burden to the drafter to show otherwise. For example, a term resulting in the transfer or assignment of ownership over IP rights that are bestowed upon the original creator, who is also the adherent, would be presumed to be unconscionable. Another example would be a term that implicitly restricts a use that is fair. The list of terms that are presumed to be unconscionable could further mirror

537. *See, e.g.*, Ohio Rev. Code § 1345.031; Mich. Comp. Laws § 445.90.

538. *See* U.C.C. § 2-719(3) (providing a term that limits business liability to death or personal injury of consumers).

539. The Restatement, *supra* note 29, at 88.

540. *See id.* at 73 (including limiting consumer’s remedies in personal injury cases or in cases the business was negligent).

541. PRINCIPLES OF THE LAW: SOFTWARE CONTRACTS § 1.11 at cmt. 1 (AM. LAW INST. 2010) (stating that § 1.11 “reproduces § 2-302 of the U.C.C.”).

542. ISRAELI STANDARD CONTRACTS LAW, § 4.

543. *Id.* at §§ 4(6), 8.

terms that were found to constitute misuse, preempted under federal law.

This proposal seeks to remedy the previously critiqued guiding principle the *Baystate* court invoked to enforce a statutory waiver. According to this principle, waivers are enforceable only when the term at hand is concerned with “protection of the property rights of individual parties . . . rather than . . . the protection of the general public.”⁵⁴⁴ In other words “‘parties may waive statutory rights granted solely for the benefit of individuals,’ but rights enacted for the benefit of the public may not be waived.”⁵⁴⁵ It cannot be disputed that fair use is a right for the benefit of the public, one that serves a clearly identifiable public policy, as do the other limiting doctrines encompassing IP’s different modes, like the idea/expression, fact/expression and first-sale doctrines. Thus, this presumption views wholesale (as opposed to “knowing, intelligent, and voluntary”)⁵⁴⁶ waivers of IP with suspicion, in line with the commonly applied principles suspicious of other waivers of statutory rights.

In fact, one court has already incorporated a similar vision under misuse, noting that a contractual term that causes users to “forego their statutorily-guaranteed right to distribute their physical copies of that same movie as they see fit” is an “improper leverage” of copyrights that “conflicts with public policy enshrined in the Copyright Act” and therefore “constitutes copyright misuse.”⁵⁴⁷ Arguably, presumptions of Unconscionability 2.0 would provide drafters with more certainty than the current regime under copyright misuse, by explicitly stating the legal regime and listing terms that warrant a higher burden of reasonableness (what Radin termed “gray listing”).⁵⁴⁸

Moreover, in one case, the Israeli Supreme Court was asked to decide if a term that conditions a dispositive statutory right, favoring the adherent, should be presumed to be unconscionable.⁵⁴⁹ While the general question remains unsettled, the Court did note that in circumstances where *multiple* provisions of *one* specific law were conditioned in a manner that negates a right given to the adherent under law, negatively affecting her position, the court should be

544. *Canal Elec. Co. v. Westinghouse Elec. Corp.*, 406 Mass. 369, 378 (1990).

545. *CSA 13-101 Loop, LLC v. Loop 101, LLC*, 236 Ariz. 410, 412 (2014) (citing *Holmes v. Graves*, 318 P.2d 354, 357 (Ariz. 1957); *Elson Dev. Co. v. Ariz. Sav. & Loan Ass’n*, 407 P.2d 930, 935 (Ariz. 1965)) (internal quotations omitted); *see also DeBerard Props. v. Lim*, 20 Cal. 4th 659, 661 (1999) (“It is true that a party may waive a statutory provision if the statute does not prohibit a waiver, the statute’s public benefit is merely incidental to its primary purpose, and waiver does not seriously compromise any public purpose that the statute was intended to serve.”).

546. *Bickel v. City of Piedmont*, 16 Cal. 4th 1040, 1043 (1997).

547. *Id.*

548. RADIN, *supra* note 1, at 231–32.

549. *Cf. CA 232/10 First Int’l Bank of Isr. v. Israeli Supervisor of Banks*, para. 28 (2012).

more suspicious in its inquiry of unconscionability.⁵⁵⁰

Indeed, similar solutions aimed at lowering litigation costs have been suggested by scholars in the context of misuse. Pallas Loren, for example, has proposed that a term that implicitly restricts a use that is fair would shift the burden of proof.⁵⁵¹ More broadly, Radin has suggested that terms that exclude users' rights (in the information made available to them) should be either subjected to "heightened scrutiny" (graylisted) or even deemed void (blacklisted), depending on extent of "social dissemination of the clauses."⁵⁵²

2. *Creating an Affirmative Right of Action*

Israel is considered a leader in policing unconscionable terms also because of its innovative judicial policing model adopted decades ago: the institutionalization of a special court designated for matters of standard form contract laws.⁵⁵³ The tribunal, mentioned in previous Sections, has authority to invalidate unconscionable terms or order that they be amended. The same authority is granted to any other civil court in Israel.⁵⁵⁴ But the tribunal is also granted broader authority: once the tribunal deems a term unconscionable (or amends the term thereof) the term is considered void (or amended) in the entire class of contracts offered by the same supplier.⁵⁵⁵

Moreover, consumer organizations and governmental bodies approved by the Israeli Attorney General, or preapproved under specific regulations,⁵⁵⁶ as well as the Israeli Consumer Authority, can file all petitions to the tribunal, requesting the review of a certain standard form contract, seeking a declaration that a term is void or should be amended.⁵⁵⁷ The tribunal can, of course, impose all litigation costs on the drafter as it sees fit.⁵⁵⁸

Finally, two of the twelve tribunal judges are designated representatives of consumer organizations, ensuring that consumers' organizations are not only able to bring contracts to the tribunal for approval and seek declaratory relief

550. *Id.* at para. 28.

551. Pallas Loren, *supra* note 46, at 535. Similarly, the notion of immunity under the recently adopted Whistleblower Immunity in the Defend Trade Secret Act entails a shift in the burden of proof, imposing the cost to prove that allowed disclosure of a trade secret was not in furtherance of an investigation of a potential violation of the law on the trade secret owner. 18 U.S.C. § 1833(b) (2018); see Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CALIF. L. REV. 1, 37–43 (2017); Peter S. Menell, *Misconstruing Whistleblower Immunity under the Defend Trade Secrets Act*, 1 NEV. L.J. F. 92, 94 (2017).

552. RADIN, *supra* note 1, at 230.

553. The Standard Contracts Law § 6 (1982).

554. *Id.* at § 3.

555. *Id.* at § 18.

556. The regulations have yet to be enacted.

557. The Standard Contracts Law at § 16(a).

558. *Id.* at § 27.

that a certain class of contracts, or their terms, are unconscionable; they also directly weigh in on decisions and how case law is shaped from the judge's seat.⁵⁵⁹

Equipped with presumptions of unconscionability, Israel's comprehensive and purposeful application of unconscionability as a doctrine, and the tribunal's broad authorities, Israeli consumers and the organizations protecting them have a broad mandate to prevent drafters from enforcing unconscionable terms. Suggesting a similar regime in the United States would probably be an impractical proposal (since contracts are matters of state and not federal law).⁵⁶⁰ Still, there are some ways to bridge the gaps between U.S. and Israeli laws. First, as other scholarship suggests, and some courts have as well, unconscionability could be reformulated as an affirmative cause of action.

Recently, Beh suggested a framework to “fortify and invigorate the unconscionability doctrine in order to promote contracting fairness in an era where one-sided, adhesionary contracts abound,” explaining that “the actual language of section 2-302 does not insist that unconscionability be merely defensive.”⁵⁶¹ The author makes suggestions and surveys other scholarly proposals to resuscitate unconscionability. These include expanding unconscionability's remedies to include restitution and reframing it as an affirmative cause of action, empowering courts to invoke unconscionability *sua sponte*,⁵⁶² shifting the burden of proof, fee-shifting, and even establishing a tort-based claim (a proposal that was recently explored by Radin) as well.⁵⁶³ I agree with Beh and Radin that fine-tuning unconscionability could enable it to fulfill its purpose. I suggest that one such improvement may include considering the policies of the contract at hand in the application of the substantive unconscionability prong.

More concretely, in matters of IP boilerplate, the arguments raised by Beh and other scholars stand on firm grounds. The costs on society imposed by contractors justify a more lenient regime and stronger deterrents, including robust remedies. In IP, courts have been using fee-shifting in copyright misuse cases to impose costs on owners who abuse their monopolistic rights,⁵⁶⁴ and

559. *Id.* at § 6(d) (added to the law in 2014).

560. *Cf.* RADIN, *supra* note 1, at 227–29.

561. Beh, *supra* note 519, at 1023 (“The distinction between defensive and offensive use is illogical and should be discarded because it may well result in only one of two similarly situated parties being unable to make use of the unconscionability doctrine.”).

562. An authority that, according to Beh, they hold under the U.C.C., although courts are indecisive on the matter. *Id.* at 1028–30. *But see* The Restatement, *supra* note 29, at 86.

563. Beh, *supra* note 519, at 1032–45; *see also* RADIN, *supra* note 1, at 198–99 (bringing forth a potential solution of a “tort of intentional deprivation of basic legal rights”).

564. *See, e.g.*, Omega S.A. v. Costco Wholesale Corp., 776 F.3d 692, 695–96; *see also* 17 U.S.C. § 505 (2018) (allowing the court discretion in awarding attorney fees to the prevailing

more generously to police abuse (sometimes amounting to “trolling”) of overarching patentees’ claims, including by non-practicing entities.⁵⁶⁵ They should be able to reach similar results in cases involving unconscionability. Consumer organizations and even administrative bodies entrusted with promoting consumer protection like the FTC, as well as bodies entrusted with promoting IP policies, such as the Copyright Office and the USPTO, should have an efficient procedure to bring forth IP boilerplate for judicial review, without relying on end-users or other entities to initiate litigation. At a minimum, boilerplate affecting a certain number of users or creators could be brought to review by these administrative bodies.

Transparency could be fostered by simply creating a database encompassing misuse, first-sale, and Unconscionability 2.0 cases affecting end-users and the language of the term in question (including a form of an accessible and searchable “black list” or “hall of shame”).⁵⁶⁶ This will bring abusive terms to the attention of consumer advocacy groups, secondary creators, and users—truly increasing terms’ salience.⁵⁶⁷

party under certain standards); *Fogerty v. Fantasy, Inc.*, 510 U.S. 517, 526–27 (1994) (interpreting 17 U.S.C. § 505).

565. *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, 134 S. Ct. 1749 (2014); Gaia Bernstein, *The Rise of the End User in Patent Litigation*, 55 B.C. L. REV. 1443 (2014); *see also* *Small v. Implant Direct Mfg. LLC*, No. 06 Civ. 683 (NRB), 2014 U.S. Dist. LEXIS 154468, *9–10 (S.D.N.Y. Oct. 22, 2014) (providing an example in the context of patent trolls: “the need for the deterrent impact of a fee award is greater where there is evidence that the plaintiff is a ‘patent troll’ or has engaged in extortive litigation”) (citing *Lumen View Tech., LLC v. Findthebest.com, Inc.*, No. 13 CIV. 3599(DLC), 2014 WL 2440867 at *7 (S.D.N.Y. May 30, 2014)); *Yufa v. TSI Inc.*, No. 09–cv–01315–KAW, 2014 WL 4071902, at *4 (N.D. Cal. Aug. 14, 2014); *see generally* Hannah Jiam, *Fee-shifting and Octane Fitness: An Empirical Approach Toward Understanding “Exceptional”*, 30 BERKELEY TECH. L.J. 611 (2015) (providing an overview).

566. *See, e.g.*, Michael, *infra* note 611, at 91–93 (suggesting that Israel adopt the publication of guidance on terms presumed to be unconscionable by market sectors, building on the UK model, and adding a simplified disclosure solution where drafters who adopt a term which is “gray listed” will need to separately disclose it in the boilerplate in a meaningful, salient way). Since the United States has yet to adopt a comprehensive model of presumptions of unconscionability, I suggest, at the first stage, building a database that will include terms that were already voided by courts (and also include terms that were voided in misuse, first-sale, and preemption cases).

567. *Cf. RADIN, supra* note 1, at 243 (noting that “NGO can organize publicity campaigns to make known to the public what some of the onerous terms in the fine print actually mean. The can take the lead in organizing a rating site that will advise consumers which firms are using reasonable terms and which are not”); *see* RANKING DIGITAL RIGHTS, <https://rankingdigitalrights.org/> [<https://perma.cc/75WY-2BXZ>] (last visited July 6, 2019) (rating leading Internet companies’ human rights accountability posture (on a variety of topics from free expression to privacy) based on their ToS and Privacy Policies, *inter alia*); *cf.* UTCCR AND THE CONSUMER RIGHTS ACT AT § 6 (2015) (enabling certain “regulators” in the United Kingdom to initiate enforcement action (a complaint) with respect to unconscionable terms);

One can even envision how such a database could be used to train machine-learning algorithms to highlight and spot unconscionable terms in the wild, and flag terms for review by consumers, regulators, and lawyers—fighting boilerplate with code, if you will. One can also envision how, in the future, these tools will also help to spot unconscionable technological boilerplate.⁵⁶⁸ And while this may sound utopian, in privacy, in the wake of public outrage over data breaches and the introduction of robust regulations like the General Data Protection Regulation (GDPR), innovators have developed machine-learning tools to flag overreaching terms and other tolls, enabling users to uncover the actual information collection practices of apps.⁵⁶⁹

3. *Some Case Studies—The Application of Unconscionability 2.0*

In previous Sections, I illustrated how Unconscionability 2.0 and presumptions of Unconscionability 2.0 could be applied to commonly used IP

see also COMPETITION & MARKETS AUTHORITY, UNFAIR CONTRACT TERMS GUIDANCE 5.7 (2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450440/Unfair_Terms_Main_Guidance.pdf [<https://perma.cc/WYL6-ZGHG>]; *see also* Michael, *infra* note 611, at 91. These bodies, as well as the UK Competition & Markets Authority, publish “Guidance” with lists of potentially unfair terms, in addition to the gray list the law provides of terms that are presumed to be unconscionable. CONSUMER RIGHTS ACT at Schedule 2, c. 15 (2015) (UK). *See, e.g.*, Gambling Commission, *Time to take action on unfair terms says Gambling Commission* (Nov. 22, 2017), <https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2017/Time-to-take-action-on-unfair-terms-says-Gambling-Commission.aspx> [<https://perma.cc/3HXZ-5X3Z>] (providing an example in gambling contracts: “terms which assume consumers have consented to the use of any personal information (including their name) for promotional purposes for the benefit of the operator”).

568. For example, machine learning is being used to spot other abusive bot-initiated behavior, such as the spread of fake news or fake endorsements. *See, e.g.*, *Fighting fake news*, BERKELEY ENGINEERING (Nov. 14, 2018), <https://engineering.berkeley.edu/magazine/fall-2018/fighting-fake-news> [<https://perma.cc/YU82-J8V6>] (describing U.C. Berkeley’s student-developed tool, SurfSafe, “a machine learning tool that helps people identify when an online photo has been doctored or is fake news”); *see also* Josh Constine, *Instagram kills off fake followers, threatens accounts that keep using apps to get them*, TECHCRUNCH (Nov. 19, 2018), <https://techcrunch.com/2018/11/19/instagram-fake-followers/> [<https://perma.cc/3M57-5D27>] (noting Instagram states they “built machine learning tools to help identify accounts that use [third-party apps for boosting followers] and remove the inauthentic activity”).

569. *See, e.g.*, Andy Greenberg, *An AI That Reads Privacy Policies So That You Don’t Have To*, WIRED (Feb. 9, 2018), <https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/> [<https://perma.cc/6FV8-JTYW>] (providing an overview of a tool called “Polisis” that enables such in the context of privacy policies); APPCENSUS, <https://appcensus.mobi/> [<https://perma.cc/FMB2-FTFG>] (reviewed in Irwin Reyes et al., “*Won’t Somebody Think of the Children?*” *Examining COPPA Compliance at Scale*, 2018(3) PROC. ON PRIVACY ENHANCING TECHS. 63 and developed by the author’s co-authors on this research) (providing an overview of a tool allowing users to search a name of a mobile app and learn about its actual information collection practices).

boilerplate language. In this Section, I will explore some additional cases studies.

If the broader reform proposals for the adoption of presumptions of unconscionability are implemented, then any term that limits a statutory right of the user, creator, or inventor under federal IP law, in a standard form contract, is presumed to be unconscionable, and therefore the burden will shift to the drafter to show that it is not unconscionable.

But even under the limiting existing framework of *Baystate* and *ProCD*, the application of Unconscionability 2.0 could garner different results. Under the first prong of procedural unconscionability, courts will inquire as to the nature of the contract and the circumstances of the parties' bargaining. As the Restatement clarifies, this is not necessarily a procedural inquiry per se focusing on notice and formation, but one that also focuses on matters of consumer awareness and issues of salience. As explained, terms relating to IP rights are often nonsalient—in other words, they do not garner the attention of consumers in a manner sufficient to affect the decision making of a substantial number of them. This is supported not only by empirical evidence but also by the fact that IP terms are “non-core” deal terms, as opposed to price,⁵⁷⁰ and because often, there is no competition in the market over the quality of IP terms. Moreover, a form contract, because of its very nature as boilerplate, is procedurally unconscionable—and the only question remaining is what level of additional “quantum” of substantive unconscionability will render it unconscionable in general.⁵⁷¹ Under the sliding scale approach, this will focus much of the inquiry on the substantive prong, a normatively desired result.⁵⁷² In the context of IP policies, this means that a term that displays a gross violation of IP objectives, like a fair use “no-parody” waiver, is unconscionable, regardless of its level of salience. By this virtue, the Israeli application of unconscionability is very much consistent with its potential U.S. counterpart.

Applying the salience principle in IP contexts will already be a step forward in reducing what I call the “dialogue of the deaf”: situations where IP scholars (or courts) seeking to promote contractual enforcement in the name of “freedom of contract” ignore the absence of such freedom in form contracts

570. See The Restatement, *supra* note 29, at 82.

571. *Id.* at 87 (“Put differently, presenting standard contract terms in a long ‘boilerplate’ may be sufficient to satisfy the procedural unconscionability prong, when a strong showing of substantive unconscionability is made.”); see also *supra* note 575 and accompanying text.

572. *Id.* at 94 (“Courts have used the ‘sliding scale’ approach to minimize the procedural unconscionability requirement and emphasize the substantive-unconscionability requirement. To maintain the dual-test doctrine, but rest it on a more coherent conceptual framework that more closely tracks the doctrine’s normative underpinnings.”).

and form contract theory. Put simply, if consumer contract law has finally come to recognize the risks imposed by form contracts and their nature, IP jurisprudence cannot continue to ignore them.

In the substantive inquiry, the court should focus on the relevant IP policies at hand and whether the term at hand displaces such policies, and may take into account other neighboring (or “core” according to some accounts) policy considerations such as free competition, free expression, or—more generally—sound public policy.⁵⁷³ Courts must look into the contract as a whole, “and the context surrounding the contract.”⁵⁷⁴ This type of (perhaps vague) inquiry is not novel. It is perhaps familiar to the reader, but under a different label or term: copyright and patent misuse, or more generally, “implied preemption.”⁵⁷⁵

Indeed, this Article does not seek to directly address the question of what should be the correct result of applying Unconscionability 2.0 to each and every case study or IP boilerplate term discussed, a question with which courts and scholars alike continue to grapple, and to which the answer might (and should) change with facts, time, and place.

The novelty of Unconscionability 2.0 is that it suggests that the current conception of the substantive unconscionability test can accommodate an inquiry into the purposes of IP policies, and that even a term that is not considered misuse or as amounting to exhaustion in a negotiated setting could be considered unconscionable once applied in at-scale form contracts. Once considered at scale, a lower quantum of substantive unconscionability is combined with an additional quantum of the procedural unconscionability that will render such term unconscionable under a sliding scale-approach. This combination allows a contextual solution to the consumer post-sale contractual enforcement question that will surely reach the courts, which explicitly takes into account the nature of boilerplate under a doctrine that is uniquely situated to evaluate boilerplate: unconscionability.

Contract law facilitates the application of other laws and policies under the substantive prong of the unconscionability analysis, although courts have yet to explicitly acknowledge that in the IP context. For example, the Restatement clarifies that “the substantive unconscionability standard may capture contract terms that are considered ‘unfair acts or practices’ under the Federal Trade Commission (FTC) Act and state Unfair and Deceptive Acts and Practices

573. Of course, these are some of the overarching policies of IP regimes. See Menell, *Economic Analysis of Network Effects*, *supra* note 116.

574. The Restatement, *supra* note 29, at 75.

575. See Rub, *Copyright Survives*, *supra* note 36; Rub, *A Less-Formalistic Copyright Preemption*, *supra* note 37; Merges, *Intellectual Property and the Costs of Commercial Exchange*, *supra* note 52, at 1613.

(UDAP) statutes,” and these statutory standards are not purely confined to policies of consumer contract law.⁵⁷⁶ This direct import of section 5 of the FTC Act into the substantive inquiry allows the FTC to take a broader role in shaping the IP boilerplate landscape within the boundaries of existing law by bringing action under the law against drafters and deployers of either IP boilerplate or unconscionable technology under the FTC’s authority.⁵⁷⁷ The ability of users and businesses to bring forth unconscionability claims against other drafters based on past complaints can complement the FTC’s enforcement power, which is often limited to egregious cases.⁵⁷⁸

Finally, if one compares Unconscionability 2.0 to Radin’s recently proposed envisioned model of unconscionability, a few points of resemblance arise. Radin brings forth an improved “tripartite evaluation” model of unconscionability that takes into account: “(1) the nature of the right; (2) the quality of consent; and (3) the extent of social dissemination of the boilerplate scheme (how many recipients are subject to it).” The third prong, she explains, is geared to ensure courts take into account that

recipients of boilerplate do not consider [some kinds of rights] important to them personally, but [these rights] are really important to civil society and the rule of law, so that the more people are burdened with deletion of such rights, the more it becomes an issue for the rule of law and for equality before the law.⁵⁷⁹

While the second prong is considered, under Unconscionability 2.0, as part of the procedural inquiry, the first and third prongs are addressed through the substantive inquiry. One potential difference is that under Unconscionability 2.0, the core of the analysis focuses on the level of democratic degradation of IP rights (in other words, displacement of IP policies) which could be facilitated, even if a very small number of recipients are subjected to the boilerplate. This is because the effects or “social dissemination” of IP boilerplate “schemes” extends well beyond the recipients (to, for example, the potential users of a fair use or commentary which is prohibited under boilerplate, or the potential secondary market of the patent or copyrighted work in case of post-sale restrictions).

576. See FEDERAL TRADE COMMISSION, FTC POLICY STATEMENT ON UNFAIRNESS (Dec. 17, 1980), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness> [<https://perma.cc/32FZ-UFM3>]; see also CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016); The Restatement, *supra* note 29, at 79–80.

577. Yet as the reporters explain, in compliance with standards does not necessarily mean a term is unconscionable and compliance with standards does not necessarily mean a term is conscionable. An analysis is needed in each case. The Restatement, *supra* note 29, at 79–80.

578. HOOFNAGLE, *supra* note 576.

579. Radin, *What Boilerplate Said*, *supra* note 55, at 5.

Let us further consider a number of case-studies, some of which I already mentioned in previous Parts, to illustrate the application of Unconscionability 2.0. Our first example is a “Single Use Only” label attached to a patent-incorporating medicine (and accompanying applicator). Below that label this text appears in fine print (on the package): “Opening this package or using the patented medicine inside confirms your acceptance of the license agreement. Following this initial use, you agree to return the empty medicine applicator only to [X-Corp] for recycling.”⁵⁸⁰ The medicine is sold in the market for over \$1,000. Another manufacturer, Y-Corp, figured out a method to replace the medicine but reuse and refurbish X-Corp applicators (disposed by consumers) in an FDA-approved non-hazardous manner. Because Y-Corp uses second-hand applicators, it can sell its medicine at a substantially lower price. But alas, the amount of available disposed applicators is limited, since consumers of X-Corp medicine are motivated (by the contract) to return them to X-Corp.

The future of Y-Corp’s secondary market is now in flux. A socially-aware group of consumers of X-Corp medicine is becoming gradually concerned with the fact the medicine, not covered by all insurers, is sold at a high price and many patients cannot afford it. Meanwhile, it is unclear if Y-Corp can continue to operate in this market amid the diluting supply of applicators. Since these consumers’ insurance only covers X-Corp medicine, they continue to buy it, but they also decide to join hands with Y-Corp in helping Y-Corp to collect applicators directly from X-Corp users, so Y-Corp can continue to operate in the market. They start to collect applicators in community meetings across the country, backed by a nationwide online media campaign calling users to bring the applicators to Y-Corp.

Following the Supreme Court decision in *Lexmark*,⁵⁸¹ Y-Corp cannot be liable under patent law for this practice. Under the broader role of exhaustion, X-Corp cannot sue its consumers under patent law. But another potential claim could be tortious interference with prospective economic relations or contractual relations against Y-Corp,⁵⁸² and of course, X-Corp can try to bring a contractual cause of action against its consumers. The question of enforceability of post-sale restrictions as a matter of contract law against consumers is still open, as explained earlier. Here, the application of Unconscionability 2.0 would provide the following results: on the procedural

580. The language above is the combination of the EULA label language used in *Lexmark* and in *Mallinckrodt*. See *Static Control Components, Inc. v. Lexmark Int’l, Inc.*, 487 F. Supp. 2d 830, 836 (E.D. Ky. 2007); *Mallinckrodt, Inc. v. Medipart, Inc.*, 976 F.2d 700, 701 (Fed. Cir. 1992).

581. *Impression Prods. v. Lexmark Int’l, Inc.*, 137 S. Ct. 1523 (2017).

582. See, e.g., *Disney Enters. v. Redbox Automated Retail, LLC*, No. CV 17-08655 DDP (AGRx), 2018 U.S. Dist. LEXIS 69103 (C.D. Cal. 2018).

inquiry, the question of the term salience should be evaluated. The disposal, single-use term seems like a non-core term for consumers. There is no competition of the quality of the term in the market since there is no other equivalent market for this medicine that allows disposal. It seems like consumers in this case must agree to terms; it is therefore nonsalient. On the question of substantive unconscionability, given that the purpose of these “patent-wrap” contracts is to limit the exhaustion doctrine and the manner consumers can use and resell a patented article, patent policy should inform the analysis whether or not such a term is unconscionable. Clearly, this term, once employed in a wholesale manner, displaces the exact same policies exhaustion seeks to advance. It is also contrary to other principles public policies seek to advance, including free competition, social justice, and access to medicine. But because this contractual language does not fall in the contours of exhaustion, courts might be reluctant to void it in a commercial, negotiated setting. Even so, the added quantum of procedural unconscionability would render the term unconscionable in a boilerplate setting, as in the case of our medicine.

Another interesting case study involves the student-(adherent)-creator. Contrary to Israeli universities, some leading world academic institutions regulate student-created innovations under a slightly more lenient regime. Among others, copyrighted software or inventions created through “significant use of funds or facilities”⁵⁸³ of the institution will be owned by the institution. Some institutions define significant use to exclude usage of facilities like libraries, computers, or general distribution of funds to students,⁵⁸⁴ while others use the term more loosely to include student stipends and “university-owned audio/visual equipment” and even “extensive use of such customarily used resources [such as library, university-owned computers, whiteboards, photocopiers, pencils, desks, and telephones]” (as opposed to routine use of such resources).⁵⁸⁵ When the student invention is created through significant use of the institution facilities, the institution may consider it owned by the

583. *Guide to The Ownership, Distribution and Commercial Development of MIT Technology*, MIT TECH. LICENSING OFF. 6, 8, https://tlo.mit.edu/sites/default/files/MIT-TLO-ownership-guide_0.pdf [<https://perma.cc/B9T8-8A4P>].

584. *Id.* at 8 (“MIT does not construe the use of office, library, machine shop or Project Athena personal desktop work stations and communication and storage servers as constituting significant use of MIT space or facilities, nor construe the payment of salary from unrestricted accounts as constituting significant use of MIT funds, except in those situations where the funds were paid specifically to support the development of certain materials.”).

585. *Intellectual Property Policy*, WILLIAM & MARY UNIV. (Mar. 9, 2016), https://www.wm.edu/offices/compliance/policies/intellectual_property/index.php [<https://perma.cc/2PZX-4PY9>].

institution.⁵⁸⁶

A broad definition of what is considered “significant use of the institution facilities” is in fact a term that could be evaluated under Unconscionability 2.0. Using this doctrine, courts can invoke IP purposes, as discussed: for example, in work-made-for-hire case law to decide the justified scope of such assignments in a boilerplate setting. Since this term is nonsalient, the focus of the inquiry would be under the substantive prong.

In other case studies, such as waivers of fair use, the terms should be presumed to be unconscionable under this proposed framework, since they limit a statutory right. The burden of proof will then reside with the drafter to show that the term is not unconscionable. It is indeed hard to imagine a limitation on fair use that is conscionable in a boilerplate, nonsalient setting. Even so, courts should use their amending prerogative under unconscionability to ensure the term is only enforced to the extent it is conscionable, in cases when a compromise is needed. To illustrate, various limitations on “tinkering” in boilerplate could be enforced only to the extent they are consistent with the DMCA good-faith security exemption limitations (that one can claim, give rise to a “statutory right” to perform security research similar to fair use).⁵⁸⁷ This interpretation would harmonize the DMCA exemption with the CFAA and contractual “anti-tinkering” regime, since once the language of an overreaching term (or deployment of blocking technology) is unconscionable, it cannot give rise to a potential CFAA liability.⁵⁸⁸ The

586. See, e.g., *Intellectual Property Policy*, WENTWORTH INST. OF TECH. <https://wit.edu/policies/intellectual-property> [<https://perma.cc/LY9G-P4TW>] (defining “Institute-Owned Intellectual Property” to include “significant use of WIT facilities, resources or equipment,” from which “use of an office, library, or desktop computer” is excluded in a policy that applies to students); see also *Intellectual Property Policy*, *supra* note 585 (providing the definition of “University Work”).

587. That is “solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.” See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 83 Fed. Reg. 540305 (2018) (to be codified at 37 C.F.R. pt. 201). The Register clarifies that the term “solely” refers to “the researcher’s purpose at the time of circumvention.” Meanwhile, post-circumvention activities, like publication of research results in academic papers or otherwise, would not exceed “the bounds of the exemption.” THE COPYRIGHT OFFICE, *supra* note 20, at 304–05.

588. In fact, in whistleblower cases courts have been invoking contractual language in employment and consultancy confidentiality agreements as void against public policy in a manner that could prevent potential CFAA liability, after the defendant (in the *Qui tam* case) brought a CFAA civil counterclaim against the whistleblower. See, e.g., *Erhart v. Bofi Holding*,

following Section will discuss the application of Unconscionability 2.0 in common settings in which other regimes (and policies) are invoked.

4. *Unconscionability 2.0 in Other Technological Realms*

Unconscionability 2.0 is not limited to IP. Boilerplate is commonly used to displace other regimes and policies, from privacy to information security and free expression. Technology can also be unconscionable, and there is a growing body of specifically opaque machine-learning and algorithmic applications that meaningfully shape, potentially in an unconscionable manner, all aspects of people's lives, sometimes perpetuating inequality and social injustices.⁵⁸⁹ As discussed, this technology operates instead of boilerplate and in conjunction with boilerplate, sometimes to enforce rights beyond what is disclosed in the ToS or even legal. If boilerplate, or technological boilerplate, is supporting unwarranted deployment of biased or deceptive machine learning processes, consumers may find additional recourse within consumer contracts law. Amid the public debate on facilitating transparency, accountability, and explainability of machine learning processes,⁵⁹⁰ unconscionability could serve as a complimentary solution to police the manner boilerplate and technological boilerplate may be deceptive, biased, operating in a socially undesired manner, or creating barriers for research and

Inc., No. 15-cv-02287-BAS-NLS, 2017 U.S. Dist. LEXIS 20959, *16–22 (S.D. Cal. Feb. 14, 2017). In other cases, they interpreted the CFAA access provisions narrowly to only apply to exceeding technological barriers. *See, e.g.,* Siebert v. Gene Sec. Network, No. 11-cv-01987-JST, 2013 U.S. Dist. LEXIS 149145 at *32–35 (N.D. Cal. Oct. 16, 2013) (finding that the whistleblower did not violate § 1030(a)(2)(C) in accessing the defendant's computer network to copy the information, since the defendant's allegations "go beyond the scope of the CFAA") (citing *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (stating that "exceeds authorized access . . . does not extend to violations of use restrictions")); *see also* Amit Elazari Bar On & Peter S. Menell, *Promoting Responsible Whistleblowing: Reconciling and Reforming CFAA Liability in the Information Age* (forthcoming) (on file with the author) (providing further discussion).

589. Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016); *see* AI Now, *Litigating Algorithms*, AI NOW INST. (Sept. 24, 2018), <https://ainowinstitute.org/announcements/litigating-algorithms.html> [<https://perma.cc/NHH9-D83B>].

590. *See* Bryan Casey et al., *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise*, 34 BERKELEY TECH. L.J. 143, 152 (2019) (claiming that "data auditing methodologies designed to safeguard against algorithmic bias throughout the entire product life cycle will likely become the new norm for promoting compliance in automated systems" and explaining how this approach is supported by the GDPR and specifically, the newly codified "right to explanation") (citing General Data Protection Regulation, 2016 O.J. (L 119) 1, Art. 22, Recital 71); Bryce Goodman & Seth Flaxman, *EU Regulations on Algorithmic Decision Making and "a Right to an Explanation"*, 38 AI MAG. 50 (2017); *see generally* Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085 (2018).

auditing.⁵⁹¹

Such barriers may include limitations on scraping, crawling, deployment of automatic tools, use of the site or services for non-personal use or research, and the like. These limitations have been the subject of at least two recent CFAA cases, where courts noted that these types of barriers to vital research could be detrimental to public policy and raise First Amendment concerns.⁵⁹² These considerations led at least two courts to decide that such limitations are unenforceable under the CFAA if they seek to limit (according to one court, even through technology) access to public websites.

Still, the contractual enforceability question remains, and it warrants a more nuanced and purposeful judicial review that can be done through unconscionability. The reason courts might seek to resort to unconscionability is the need to limit the question of enforceability strictly to boilerplate settings. Private parties might still agree, in truly freely negotiated contracts and commercial settings, they want to limit reverse engineering, tinkering, decompiling, and other research activities. While these provisions may limit the ability of competitors (that sometimes emerge as potential whistleblowers and perform effective auditing),⁵⁹³ to contribute to the auditing efforts, or even to expose potential illegal activity facilitated through technology, there could be reasonable business rationales, such as trade secrecy protection, for their enforcement in negotiated, salient contracts. Still, these provisions' effect is

591. Algorithmic Auditors are a growing discipline of researchers in computer science and human-computer interaction (HCI) that employ a variety of methods to tinker and uncover how algorithms work. Their work has already sparked public discussions and regulatory investigations into the most dominant algorithms of the information age. See Christian Sandvig et al., *Auditing algorithms: Research methods for detecting discrimination on internet platforms*, 2014 DATA AND DISCRIMINATION: CONVERTING CRITICAL CONCERNS INTO PRODUCTIVE INQUIRY 1; Amit Elazari Bar On, *We Need Bug Bounties for Bad Algorithms*, MOTHERBOARD VICE (May 3, 2018), https://motherboard.vice.com/en_us/article/8xkyj3/we-need-bug-bounties-for-bad-algorithms [<https://perma.cc/5DKQ-725T>]; see also Motahhare Eslami et al., *User Attitudes towards Algorithmic Opacity and Transparency in Online Reviewing Platforms*, in CHI '19 PROC. 2019 CHI CONF. ON HUM. FACTORS IN COMPUTING SYS. (2019).

592. See Sandvig v. Sessions, No. 16-1368 (JDB), 2018 U.S. Dist. LEXIS 54339 (D.D.C. Mar. 30, 2018); hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099 (N.D. Cal. 2017), *aff'd*, No. 17-16783, 2019 WL 4251889 (9th Cir. Sept. 9, 2019) (“[G]iving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest.”); Komal S. Patel, *Testing the Limits of the First Amendment: How Online Civil Rights Testing is Protected Speech Activity*, 118 COLUM. L. REV. 1473 (2017) (providing a discussion in the interaction of algorithmic auditing with first amendment concerns and the CFAA).

593. See Annie Lee, *Algorithmic Auditing and Competition Under the CFAA: The Revocation Paradigm of Interpreting Access and Authorization*, 33 BERKELEY TECH. L.J. 1307 (2018).

less impactful than overreaching boilerplate applying to all users of a service, platform, or technology, including academic researchers. Moreover, there are other tools that could be applied to prevent negotiated contracts from stifling whistleblowing or competition.⁵⁹⁴

Unconscionability 2.0 can be used in this context to allow different results for different contracts in cases that will not fit under the contours of clear statutory limitations on boilerplate such as the new anti-disparagement Consumer Review Fairness Act. It can also be used to evaluate technology, as discussed in previous Sections.

Moreover, the same Unconscionability 2.0 framework can be applied to provisions that undermine cybersecurity and privacy policies. These may include boilerplate allowing the manufacturer, the website, or an app unlimited permissions, well beyond what users expect is needed to operate the service or other practices that were found to be “unreasonable” under the FTC Act.⁵⁹⁵ The added value from disciplining such provisions under unconscionability is the ability to bring forth a private right of action for a broader set of practices that may not be covered under existing regulation. The core function of Unconscionability 2.0 in these contexts is to ensure that courts consider the purposes of these regimes when inquiring into the substantive unconscionability prong, and not be limited to questions of “price” and “meaningful choice.”

Courts should also be mindful of the fact that one provision, (for example, “no bots or automatic tools allowed”),⁵⁹⁶ or technology (blockers that enforce this example of anti-bot ToS provision),⁵⁹⁷ may interact with more than one regime, and all such policies should be considered, even if they do not arise from the factual circumstances at hand. For example, an anti-bots boilerplate in a public website can limit privacy, security, and algorithmic auditing, but it can also limit transformative fair use.⁵⁹⁸

594. Such as the Defend Trade Secret Act Whistleblower immunity. *See supra* note 551. Yet this provision does not provide immunity from the CFAA. *See* 18 U.S.C. § 1833(b)(5) (2018); *see also* Peter S. Menell, *The Defend Trade Secrets Act Whistleblower Immunity Provision: A Legislative History*, 1 BUS. ENTREPRENEURSHIP & TAX L. REV. 399, 422 (2017); Elazari Bar On & Menell, *supra* note 588. Antitrust also provide a variety of tools. *See, e.g.*, Maureen A. O’Rourke, *Striking a Delicate Balance: Intellectual Property, Antitrust, Contract, and Standardization in the Computer Industry*, 12 HARV. J.L. & TECH. 1 (1998).

595. *See, e.g.*, *In re Goldshores Techs. LLC & Erik M. Geidl*, FTC File No. C-4446 (F.T.C. 2014); CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016), at ch. 6, 8; *see also* RADIN, *supra* note 1, at 176–79.

596. *See Sandvig*, 2018 U.S. Dist. LEXIS 54339, at *27, *48.

597. *hiQ Labs*, 273 F. Supp. 3d at 1103.

598. *See* Authors Guild v. Google, Inc., 804 F.3d 202 (2d Cir. 2015).

Finally, as explained, the application of competing values and policies could be done under Unconscionability 2.0 and within its boundaries. In fact, that is how Israeli courts have been evaluating unconscionability for the past four decades, as part of the Israeli application of the purposive approach.

5. *Unconscionability 2.0: A “Wild Card” or a Winning Hand—Some Objections and Responses*

At various junctions throughout this Article, I raised some potential arguments that could be claimed against the proposed application of Unconscionability 2.0. I attempted to address them as they arose, and in the context discussed, but still it is useful to summarize some of the core critiques and potential responses.

One prominent critique that the proposed application of unconscionability raises, especially in cases that leave unfettered discretion for courts to consider public policy considerations within their boundaries, is its uncertainty and vagueness. Indeed, opponents of unconscionability have been voicing such concerns for decades.⁵⁹⁹ But as I mentioned—and other scholars (and courts) have argued at length⁶⁰⁰—it is exactly that flexibility and vagueness that allows unconscionability to operate effectively.

Unconscionability, like other common law doctrines such as the duty of good faith, public policy exception, and equitable defenses such as misuse and unclean hands, are tools geared to deal with uncertain circumstances, changes (including technological ones), and shifting cultural and societal perceptions.⁶⁰¹ The common law relies on their application as such.⁶⁰² Specifically, unconscionability’s potency lies in its vagueness because it is unreasonable to assume any regulator or legislator can anticipate all forms and shapes of private parties’ potentially abusive drafting and contracting behaviors to the extent needed to create specific rules against them.⁶⁰³ In fact, given their prominence, it is unreasonable even to assume any regulator can read or collect these

599. Evelyn L. Brown, *The Uncertainty of U.C.C. Section 2-302: Why Unconscionability Has Become a Relic*, 105 COM. L.J. 287, 293 (2000).

600. M. P. Ellinghaus, *In Defense of Unconscionability*, 78 YALE L.J. 757, 795 (1969) (explaining that unconscionability is part of contract law’s “residual categories,” categories of doctrines that operate under necessary vagueness such as “reasonableness,” “due care,” and “good faith”). Israeli unconscionability is also considered a standard, an indented instance of a “valve concept” (Ventilbegriffe), the content of which is always changing with time and according to circumstances and ever-evolving worldviews. See *supra* notes 472–474 and accompanying text.

601. Shyamkrishna Balganesh, *The Pragmatic Incrementalism of Common Law Intellectual Property*, 63 VAND. L. REV. 1543, 1568 (2010).

602. *Id.*

603. See RADIN, *supra* note 1, at ch. 12.

contracts, let alone scrutinize them in a comprehensive manner. Ellinghaus foresaw this reality, noting as far back as 1969 that “[u]nconscionability is a ‘standard’ which awaits, and is designed to encourage, organic development by the courts,” a necessary category of “shifting content and expansible nature,” that “[w]e cannot do without.”⁶⁰⁴

The core hostility towards unconscionability raised by the Chicago School of Law and Economics theorists is that such uncertainty may interfere in what would otherwise be an efficient economy, facilitated by freedom of contracts and competition.⁶⁰⁵ But as I have shown, even under this (arguably narrow) vision of unconscionability, such considerations are taken into account under the procedural inquiry as to the salience of the term. The consideration of procedural unconscionability (even to a minimal extent and under a sliding scale approach), allows a court to decide whether there is, in fact, a need to intervene and police terms (that are not policed in the market). To some extent, this combination makes Unconscionability 2.0 more sensitive to these arguments than doctrines such as copyright misuse that are not focused on such considerations.

Still, and as I explained, IP boilerplate terms are not ordinary commercial terms. They create externalities, displace IP policies, and impose societal costs. In this context, Radin’s arguments against reduction of “all human activity to private market activity,[] all values to price,” “and all ordering to private ordering” ring true.⁶⁰⁶ In fact, Unconscionability 2.0 reaches beyond traditional economic analysis, and accounts for what Radin calls the “normative degradation” effect of boilerplate.⁶⁰⁷ Matters of price and efficiency are not identical to matters of autonomy, personhood, and justice, and the displacement of IP policies has a cost that cannot simply be reduced to matters of efficiency. That is why, in IP, scholars are still debating over the correct framework (or better yet frameworks) to apply, irrespective of questions of contract enforcement.

While a full discussion in these two philosophical debates, the one between so-called “Chicagoans” and “autonomists” in boilerplate theory,⁶⁰⁸ and the one

604. Ellinghaus, *supra* note 600, at 814–15.

605. See *supra* note 252; Radin, *What Boilerplate Said*, *supra* note 55, at 8 (“[T]he business will save money by deleting its consumers’ legal rights; the business will pass on these savings to the consumer; the consumer who buys the product or service necessarily values her legal rights less than the amount of the price reduction; therefore the consumer is choosing (or should be assumed to be ‘rational’ and therefore hypothetically to choose) to sell off her individual rights for the price reduction.”).

606. *Id.* at 10–11.

607. See *supra* note 579 and accompanying text.

608. Omri Ben-Shahar, *Regulation Through Boilerplate*, *supra* note 3, at 884–85; Radin, *What Boilerplate Said*, *supra* note 55.

between so-called “utilitarian” and “exutilitarian” in IP policy,⁶⁰⁹ is beyond the scope of this Article, Unconscionability 2.0 seems to be able to accommodate both frameworks. Even those taking a narrower view on boilerplate enforceability would agree that at minimum, the nature of the contract (as regulating IP rights) should be taken into account, that some market failures are not solved in the market,⁶¹⁰ and that IP regimes, jurisprudence, and tradition are better equipped to recognize market failures that fall within their realms than vaguely applied concepts of price and sale that have little to do with the facts or contract at hand.

Finally, it is important to recognize that the concerns voiced by those opposing vague application of unconscionability seem to not be supported by empirical evidence.⁶¹¹ In other words, the so-called costs of said uncertainty do not seem to limit the application of boilerplate or hinder its economic benefits. Boilerplate is very much “alive and kicking,” including in jurisdictions with a robust black letter law vision of unconscionability, such as Israel. It could be claimed that the low probability (P) of litigation serves as balancing criteria against the costs of an unjustified unconscionable judicial decision (L).⁶¹² In other words, drafters are not really policed, even in jurisdictions that adopted a robust view of unconscionability, from including unconscionable terms in their contracts, because the only remedy is unenforceability (and in Israel, for example, fee shifting), and there is a low probability of litigation or regulatory enforcement. That is why I (and others) suggested that P should be increased by adopting a more robust model of unconscionability, and more remedies should be considered to create a deterrent effect. Furthermore, the costs of market uncertainty in the context of IP policies ought to be considered against the societal costs imposed by IP boilerplate abusive to IP rights, and the broader societal uncertainty from failing to police such abuses. These uncertainties should also be evaluated against the currently available solutions: most prominently, misuse.

While I don’t have empirical evidence to support this proposition, I would argue that some limited uncertainty experienced by private parties as to their ability to enforce their unilaterally drafted rights is a lesser problem than the

609. See *supra* note 492 and accompanying text.

610. The Restatement, *supra* note 29, at 94; see also Korobkin, *supra* note 74.

611. If anything, evidence supports the contrary: that some “exculpatory clauses [eliminating tort claims] create a massive moral hazard problem,” that is not controlled by the market. See Radin, *What Boilerplate Said*, *supra* note 55, at n.11; RADIN, *supra* note 1, at 139–40.

612. Liran Michael, *Getting to the Trough but not Drinking the Water: The Failure of the Standard Contracts Law and Proposals For Change*, 5 HUKIM (LAWS) 59, 73 (2013) (In Hebrew). The title is a paraphrase on an old Hebrew dictum, “you can get the horses to the trough, you cannot force them to drink the water”—in other words, while the law has robust provisions, it does not guarantee consumers will actually make use of such provisions.

uncertainty of society at large as to the rule of law and the broader application of IP law, and uncertainty about whether the market polices IP boilerplate adequately or not.⁶¹³ Maybe that is why, even though misuse is also often critiqued for its “uncertainties” and “vagueness,”⁶¹⁴ it is still applied by courts, and recently even more rigorously. Put simply, reality proves that we still need common law vague concepts to deal with contractual abuse (and the boilerplate drafters who contributed to it) in the IP setting, and if we still need such concepts, we might as well adopt them to better fit their purpose in the boilerplate setting.

I have also suggested pathways to mitigate such uncertainness, including by incorporating presumptions of unconscionability and creating databases of unconscionable terms. One can even envision a procedure that will allow an especially risk-averse private party to petition for a declaratory relief that its contract is enforceable.⁶¹⁵ In Israel, such procedure existed for decades, until 2014. The tribunal could have “preapproved” a standard form contract, granting the boilerplate near-immunity from unconscionability claims for a five-year period, and removing any uncertainty as to the enforceability of the term.⁶¹⁶ The “proud” drafter could even label its form contract as “approved” by the tribunal. This procedure was canceled and removed from the law in 2014, after it was found to be ineffective.⁶¹⁷ Empirical research showed that over a period of fifteen years (1996–2011), on average, only two approval requests were filed in Israel per year, a total of thirty requests over a decade and a half.⁶¹⁸ At least in Israel, or so it seems, boilerplate drafters preferred to remain uncertain than to risk that terms would be voided or changed.

613. Cf. RADIN, *supra* note 1, at 164 (“Even if people do mean to assume the risks posed by boilerplate clauses, we should understand that they are likely to be mistaken about the level of risk that they face . . .”).

614. See *Lasercomb Am., Inc. v. Reynolds*, 911 F.2d 970, 973 (4th Cir. 1990); see also Troy Paredes, *Copyright Misuse Tying: Will Courts Stop Misusing Misuse*, 9 HIGH TECH. L.J. 271 (1994); Kathryn Judge, *Rethinking Copyright Misuse*, 57 STAN. L. REV. 901 (2004) (discussing such arguments).

615. Cf. Clayton P. Gillette, *Pre-Approved Contracts for Internet Commerce*, 42 Hous. L. Rev. 975 (2005) (suggesting a pre-approval process for “contracts” to be administrated by a federal agency); RADIN, *supra* note 1, at 227–29 (discussing this proposal).

616. See The Standard Contracts Law, ch. C §§ 12–15 (1982) (Isr.). Under unique justified circumstances and the request of the Israeli Attorney General, the tribunal could still void a term in a preapproved contract. *Id.* at § 14(c); see Deutch, *Controlling Standard Contracts*, *supra* note 423.

617. Proposed Bill to amend the Standard Form Contract Law, Amend. n.5 at p. 296–97 (2014) (in Hebrew); cf. Gillette, *supra* note 615 (noting that “sellers will not necessarily take advantage of the [pre-approval] process”).

618. Michael, *supra* note 612, at 72.

Another potential critique could be that other doctrines might better serve the purpose of policing boilerplate terms that are abusive to IP policies. These doctrines include the public policy exception in contract law, and misuse, implied preemption, and in some cases, first-sale or exhaustion in IP. I discussed this critique in Section II(F). In a nutshell, this critique is warranted. Unconscionability 2.0 is not an exclusive solution. As explained, Unconscionability 2.0 is best equipped to cabin questions of boilerplate enforceability (such as salience) and IP policies within the same doctrine, and therefore allows a contextual approach that can distinguish between negotiated and unnegotiated contracts. Moreover, as I claimed, at least in its modest version, Unconscionability 2.0 is an accessible solution that does not further require reform. With the adoption of the Restatement, and the proliferation of IP boilerplate, courts will be invited to apply the reconceptualized vision of unconscionability in IP cases. They can use this opportunity to adopt a purposeful use of unconscionability that combines IP considerations: Unconscionability 2.0. This path to police contracts seems more sustainable than hoping that the “no-preemption” vision of contracts, applied in almost all circuits of the United States,⁶¹⁹ would be reversed in those circuits.

Finally, another critique is that Unconscionability 2.0 could invite conflicting applications across the United States since contracts are a matter of contract law, while IP is governed under federal law. Already, unconscionability has different interpretations in different states under contracts,⁶²⁰ which makes the doctrine potentially too unstable to also deal with matters of IP. But misuse also has different interpretations, and so does preemption. That is the nature of common law: to create different results until coherency is achieved, reality (and technology) warrants a different result, and again the vicious cycle repeats.⁶²¹ Usually Unconscionability 2.0 claims, similar to misuse claims, would be litigated in federal courts (because another IP claim would be raised) which are well-equipped to decide on both matters of IP policy and unconscionability. In the rare case that they not, one can suggest that Unconscionability 2.0 claims would be litigated in federal courts.

619. Rub, *Copyright Survives*, *supra* note 36.

620. See The Restatement, *supra* note 29, at § 5.

621. Balganes, *supra* note 601, at 1615 (“[T]he method of lawmaking that common law [in IP] emphasizes the virtues of beginning the process without looking to an abstract theory to justify the outcome, of focusing on the context for a rule, of understanding the short- and long-term consequences of a rule, and of proceeding with caution, one case at a time.”); see Shyamkrishna Balganes, “The Common Law” *In the Law and Economics of Intellectual Property*, in RESEARCH HANDBOOK ON THE ECONOMICS OF INTELLECTUAL PROPERTY LAW (VOL. I, THEORY) (Peter S. Menell & Ben Depoorter eds., forthcoming 2019).

V. CONCLUSION

The year is 2040. Code is law, design is governing,⁶²² and all contracts are “smart.”⁶²³ Almost everything is intangible, connected, or “intellectual.” All U.S. law schools teach Intellectual Property and Technology Law in multiple core mandatory classes, alongside coding, since it is the most prominent legal regime affecting commerce and economic growth across the globe. The traditional mode of contracting is displaced by digital handshakes rigorously enforced by technology. Society is struggling to keep technology in check and accountable. Is this a dystopian vision or one grounded in reality? This Article suggests that the law is still failing to address problems created by boilerplate in IP realms and that unconscionability could be an accessible solution if interpreted purposefully to accommodate IP considerations under the substantive prong.

Currently, private ordering, facilitated by either contract or technology, is rarely regulated in the context of IP. Arguably, we might have more boilerplate regulation of creations and innovations than statutory rights. We enforce boilerplate that limits fair use rights and allows the deployment of algorithms that falsely remove content and code that limits users’ access, copying, or scraping across every dark corner of the web and the connected world.

Lessig once spoke of the astounding irony that often characterizes the struggles within IP realms, claiming that we “move through this moment of an architecture of innovation to, once again, embrace architecture of . . . control . . . without resistance.”⁶²⁴ He further notes that “[t]hose threatened by this technology of freedom have learned how to turn the technology off.” He asserts that “[t]he switch is now being thrown” and “[w]e are doing nothing about it.”⁶²⁵

If the law cannot develop to limit the abusive application of boilerplate, how can it develop to deal with boilerplate’s more developed and powerful successor, code?⁶²⁶ And if law is already displaced by contracts that we can

622. Mulligan & Bamberger, *supra* note 174.

623. Adam J. Kolber, *Not-So-Smart Blockchain Contracts and Artificial Responsibility*, 21 STAN. TECH. L. REV. 198, 199 (2018) (outlining the “broader danger lurking in the code-is-the-contract view”); *see also* Kieron O’hara, *Smart Contracts-Dumb Idea*, 21.2 IEEE INTERNET COMPUTING 97, 100 (2017) (explaining that “[j]ust because we can imagine different types of mechanisms being used to constrain behavior, it doesn’t follow, as many assume, that these mechanisms are interchangeable” and reviewing some consequences of replacing law with software).

624. LAWRENCE LESSIG, *THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD* 267–68 (2002).

625. *Id.*

626. RADIN, *supra* note 1, at 46.

read, how can we prevent a reality in which opaque technology is displacing it? Unconscionability 2.0 is not a panacea and has its limitations. But as Radin puts it, “doing nothing about the current [boilerplate] situation is not a panacea either.”⁶²⁷ If we are not willing to pull the switch on contractual boilerplate, we will find it harder to regulate technology when it is operating as boilerplate, a future that is unclear if society can afford.⁶²⁸ Our hand is on the switch, and in Unconscionability 2.0 we have an accessible solution at hand. We just need to replace the formalistic and ineffective doctrine of Unconscionability 1.0 with the inter-doctrinal, flexible, and purposeful solution of Unconscionability 2.0.

627. *Id.* at 229.

628. *See* Mulligan & Bamberger, *supra* note 174.

