

36:1 BERKELEY TECHNOLOGY LAW JOURNAL

2021

Pages

305

to

616

Berkeley Technology Law Journal

Volume 36, Number 1

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 © 2021 Regents of the University of California.
All Rights Reserved.

Berkeley Technology Law Journal
University of California
School of Law
3 Law Building
Berkeley, California 94720-7200
editor@btlj.org
<https://www.btlj.org>



BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 36

NUMBER 1

2021

TABLE OF CONTENTS

ARTICLES

| | |
|---|-----|
| PRIVACY SELF-HELP | 305 |
| <i>Steven H. Hazel</i> | |
| ANTITRUST IN THE CONSUMER PLATFORM ECONOMY: HOW APPLE HAS ABUSED ITS MOBILE PLATFORM DOMINANCE | 353 |
| <i>Shili Shao</i> | |
| WHY 72 INTELLECTUAL PROPERTY SCHOLARS SUPPORTED GOOGLE'S COPYRIGHTABILITY ANALYSIS IN THE ORACLE CASE..... | 413 |
| <i>Pamela Samuelson & Catherine Crump</i> | |
| TRADEMARKS AS SURVEILLANCE TRANSPARENCY..... | 439 |
| <i>Amanda Levendowski</i> | |
| PLATFORMS, ENCRYPTION, AND THE CFAA: THE CASE OF <i>WHATSAPP V.</i> <i>NSO GROUP</i> | 469 |
| <i>Jonathon W. Penney & Bruce Schneier</i> | |
| A PENNY FOR THEIR CREATIONS—APPRIISING USERS' VALUE OF COPYRIGHTS IN THEIR SOCIAL MEDIA CONTENT | 511 |
| <i>Uri Y. Hacohen, Amit Elazari & Talia Schwartz-Maor</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 36 BERKELEY TECH. L.J. ____ (2021).

BTLJ ONLINE

The full text and abstracts of many previously published *Berkeley Technology Law Journal* articles can be found at <https://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://btlj.scholasticahq.com/for-authors>.

Citations. All citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 21st ed. 2020).

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

WHITE & CASE LLP

Benefactors

BAKER BOTTS LLP

MORRISON & FOERSTER LLP

COVINGTON & BURLING LLP

ORRICK HERRINGTON & SUTCLIFFE
LLP

FENWICK & WEST LLP

PAUL HASTINGS LLP

FISH & RICHARDSON P.C.

SIDLEY AUSTIN LLP

KIRKLAND & ELLIS LLP

WEIL, GOTSHAL & MANGES LLP

LATHAM & WATKINS LLP

WILMER CUTLER PICKERING HALE
AND DORR LLP

MCDERMOTT WILL & EMERY LLP

WILSON SONSINI GOODRICH &
ROSATI

WINSTON & STRAWN LLP

Corporate, Government, Individual, and Foundation Sponsors

| | |
|------------------------------|---------------------------|
| ATLASSIAN | LITINOMICS, INC. |
| BOIES SCHILLER & FLEXNER LLP | MARKS & CLERK LLP |
| CISCO SYSTEMS, INC. | MICROSOFT CORPORATION |
| THE CITIZEN LAB | MOZILLA CORPORATION |
| COMCAST CABLE | NOKIA CORPORATION |
| CORNERSTONE RESEARCH | PALANTIR TECHNOLOGIES |
| DARTS IP | QUALCOMM INCORPORATED |
| GEN LAW FIRM | RLM TRIALGRAPHIX |
| GOODWIN PROCTER LLP | STARZ |
| GOOGLE INC. | TYSON & MENDES |
| INTEL CORPORATION | UNIFY CONSULTING |
| INVENTIONSHARE INC. | VIA LICENSING CORPORATION |
| JENNER & BLOCK | VYNL |
| KILBURN & STRODE | WESTERN DIGITAL |

Members

BAKER & MCKENZIE LLP

KILPATRICK TOWNSEND &
STOCKTON LLP

BEIJING EAST IP

KNOBBE MARTENS LLP

DESMARAIS LLP

MORGAN LEWIS & BROCKIUS

DURIE TANGRI LLP

ROBINS KAPLAN, MILLER & CIRESI
LLP

GREENBERG TRAURIG LLP

TENSEGRITY LAW GROUP LLP

GTC LAW GROUP LLP & AFFILIATES

VAN PELT, YI & JAMES LLP

HAYNES AND BOONE, LLP

WANHUIDA INTELLECTUAL
PROPERTY

IRELL & MANELLA LLP

WILLKIE FARR & GALLAGHER LLP

KEKER VAN NEST & PETERS LLP

WOMBLE BOND DICKINSON LLP

BOARD OF EDITORS

2020–2021

Executive Board

Editor-in-Chief
S. EMMA LEE

Senior Articles Editors
MUHTADI CHOUDHURI
MATT CHUNG
MARTA ROCHA

Senior Executive Editor
HARRISON GERON

Senior Production Editor
HAILEY YOOK

Managing Editor
MADISON BOWER

Senior Scholarship Editor
ANGELA GRIGGS

Senior Student Publication Editors
WALTER MOSTOWY
KEVIN YANG

Senior Online Content Editor
ALLAN E. HOLDER

Editorial Board

Submissions Editors
JOHN BATOHA
GRACE MCFEE
THOMAS HORN

Production Editors
ROBIN CHANG
JOELLE FERGUSON
EMILY ROBERTS

Technical Editors
SALLY CHOI
MIN JUNG “MJ” HAN
ALEX HARVEY
JOSEPH KINGERSKI

Student Publication Editors
JENNIFER CHUNG
ANUJ EZEKIEL

Notes & Comments Editors
LOC HO
SHREYA SANTHANAM

Symposium Editors
MARGARET LYNCH
DEBBIE MOSLEY

Web & Technology Editors
KARNIK HAJJAR
HENRY METRO

Podcast Editors
HALEY BROUGHTON
ANDY ZACHRICH

LLM Editor
MARIO MARTINEZ

Member Relations Editor
RACHEL WILSON

Alumni Relations Editor
ARMBIEN SABILLO

External Relations Editor
GRACE (HJ) KIM

Commentaries Editor
VERONICA BOGNOT

Articles Editors
LIAM AZARTASH
KEVIN CHEN
NATALIE T. CRAWFORD
JAMESON DAVIS
JASON FRANCIS

Articles Editors
JEFFREY JACOBSEN
TOM JAMES
JOSEPH KROON
CHARLIZE MORGAN
ALEX MCKENZIE
SHALEV NETANEL

Articles Editors
YEMAJ SHEIK
DAKOTA SNEED
BLAINE VALENCIA
SOPHIA WALLACH
ALI ZARRABI

MEMBERSHIP

Vol. 36, Design Patents Symposium

Associate Editors

| | | |
|-----------------|--------------------|--------------|
| JONATHAN BAER | KAVYA DASARI | FATIMA LADHA |
| BOGDAN BELEI | KURT FREDERICKSON | WYATT LARKIN |
| SETH BERTOLUCCI | RAFI GINSBURG | MATT SARDO |
| CONNOR BOEHM | REBECCA HO | SARA TSAI |
| HALEY BROUGHTON | NATHANIEL KELLERER | JESSICA WANG |
| LUCILLE DAI-HE | CONNOR KENNEDY | |

Members

| | | |
|---------------------------|--------------------|----------------------------|
| JARED ABES | EDUARDO FIGUEROA | ROSS MOODY |
| RICH ABIDOR | COLE GINGRICH | ERIN MOORE |
| IAN AFLAGUE | KHASH GOSHTASBI | GAYATRI PARANJAPE |
| TIFFANY ALLEN | SAVANNAH GROSSARTH | JUSTINE MCCARTHY POTTER |
| SCOTT ARONIN | DYLAN HOULE | BREANNA QIN |
| PIERRE BARTHELEMY | CHRISTINA JOHNSON | JENNY QUANG |
| MIKE BEHLEN | NATALIE KALISS | MEIRAM RAKHIMBEKOV |
| BROOKE D'AMORE BRADLEY | ROGER KANG | LIZ FREEMAN ROSENZWEIG |
| HANNAH BROWN | CHRISTIAN KNIPFER | BARBARA ROWINSKA |
| ZHIWEI CAI | PAULINE LE | CATIE SAKURAI |
| KEVIN CHIU | DIANA LEE | WILL SERIO |
| MACKENZIE CONCEPCION | GARY LEE | EVA SPITZEN |
| ALEXA DAUGHERTY | VALENTINO LUCINI | MEGHAN SULLIVAN |
| VICTORIA DIPLA | MATTHEW LUEVANO | JENNIFER SUN |
| MADELINE ELKINS | MAHAA MAHMOOD | RACHEL THOMPSON |
| CLINTON EWELL | BLAINE MANIRE | MICHELLE WONG |
| ROBERT FAIRBANKS | THOMAS MATTES | DIMING XU |
| CITRA FATIHAH | ISHITA MATTOO | ANGELA ZHAO |
| KAYLA FEDLER | ALISTAIR MCINTYRE | MICHELLE ZIPERSTEIN |
| | DANIEL METEER | |

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
*Richard M. Sherman Distinguished 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
*Professor of Law, Emeritus and Director of the
International Entertainment & Media Law
Summer Program in London*
Southwestern University 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
*Assistant 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 2020–2021

Executive Director

JIM DEMPSEY

Faculty Directors

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

Fellow

| | |
|-------------------|----------|
| KATHRYN HASHIMOTO | YUAN HAO |
|-------------------|----------|

Staff

| | |
|-----------------|---------------|
| MARK COHEN | RICHARD RISK |
| NATALIE COLETTA | MATTHEW RAY |
| JANN DUDLEY | IRYS SCHENKER |

PRIVACY SELF-HELP

Steven H. Hazel[†]

ABSTRACT

Today, millions of consumers practice privacy self-help. Some cover their laptop cameras; others communicate through encrypted messaging apps; still others delete sensitive documents. But while self-help has emerged as one of the primary ways that consumers manage privacy risks, it has attracted little scholarly attention.

To fill that gap, this Article offers a descriptive account of the relationship between privacy doctrine and self-help. As it turns out, privacy law relies on self-help to solve some of its most pressing problems. From the Fourth Amendment to the FTC's unfairness authority, courts and regulators look to self-help to decide which disputes deserve attention and to conserve scarce resources. The upshot is that harnessing self-help has become a pervasive feature of modern privacy law.

Turning from the descriptive to the normative, this Article asks how law should respond to privacy self-help. Too often, self-help exposes the data it promises to protect. When self-help backfires, the conventional wisdom holds that courts and regulators should install legal remedies to replace it. But displacing self-help would disable the doctrines that depend on it.

Challenging the conventional wisdom, this Article shows that legal institutions protect consumers best when they facilitate—rather than replace—self-help. By arming individuals with intelligence about self-help, courts and regulators can empower them to spot successful strategies and sidestep self-defeating ones. This approach promises to transform self-help from a popular yet unreliable practice into a potent weapon in the hands of millions of consumers. Ultimately, complementing self-help should be privacy law's first instinct, not its last resort.

TABLE OF CONTENTS

| | | |
|-------------|---|------------|
| I. | INTRODUCTION | 307 |
| II. | SELF-HELP IN PRACTICE..... | 310 |
| | A. DEFINING SELF-HELP..... | 311 |
| | B. SURVEYING SELF-HELP | 312 |
| | 1. <i>Concealment Strategies</i> | 313 |
| | a) Concealing Identifying Information..... | 314 |
| | b) Concealing Sensitive Information | 315 |
| | c) Concealing Previously-Disclosed Information..... | 316 |
| | 2. <i>Obfuscation Strategies</i> | 318 |
| | a) Obfuscating Identifying Information..... | 318 |
| | b) Obfuscating Sensitive Information | 319 |
| | c) Obfuscating Activity | 320 |
| | 3. <i>Monitoring Strategies</i> | 321 |
| | a) Personal Monitoring | 321 |
| | b) Monitoring Services | 322 |
| | c) Monitoring Networks | 323 |
| III. | THE PERILS OF SELF-HELP | 324 |
| | A. PRIVACY-PRIVACY TRADEOFFS..... | 325 |
| | 1. <i>Self-Help as Data Creation</i> | 326 |
| | 2. <i>Negative Inferences</i> | 327 |
| | 3. <i>Overreliance</i> | 328 |
| | B. SECURITY-PRIVACY TRADEOFFS..... | 328 |
| | 1. <i>Confidentiality</i> | 329 |
| | 2. <i>Integrity</i> | 330 |
| | 3. <i>Availability</i> | 331 |
| | C. ARMS RACES | 332 |
| | 1. <i>Surveillance Technologies</i> | 333 |
| | 2. <i>Data Brokers</i> | 334 |
| IV. | HOW PRIVACY LAW HARNESSSES SELF-HELP | 335 |
| | A. THE FOURTH AMENDMENT..... | 336 |
| | B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT | 336 |
| | C. ARTICLE III STANDING IN DATA BREACH CASES..... | 337 |
| | D. PRIVACY TORTS | 338 |
| | E. DATA BREACH NOTIFICATION STATUTES | 340 |
| V. | THE CASE FOR COMPLEMENTING SELF-HELP | 341 |
| | A. HOW LAW CAN COMPLEMENT SELF-HELP | 342 |

| | | |
|-----|---|-----|
| 1. | <i>Revisiting Generally Applicable Laws That Exacerbate Asymmetries</i> ... | 342 |
| 2. | <i>Extracting Intelligence from Data Processing Firms</i> | 345 |
| 3. | <i>Disrupting Invisible Arms Races</i> | 347 |
| B. | COMPLICATIONS..... | 349 |
| 1. | <i>The Gap Between Information and Action</i> | 349 |
| 2. | <i>The Social Costs of Self-Help</i> | 350 |
| 3. | <i>The Market Alternative to Self-Help</i> | 351 |
| VI. | CONCLUSION..... | 352 |

I. INTRODUCTION

Mark Zuckerberg, Facebook’s founder and CEO, is not generally regarded as a privacy advocate. In 2010, for instance, he proclaimed that privacy is no longer “a social norm.”¹ But photos indicate that Zuckerberg may be more concerned about privacy than his public statements suggest. Zuckerberg—a Harvard-trained computer scientist who employs thousands of engineers—covers his MacBook’s camera with a piece of tape.² And Zuckerberg isn’t the only one.³ Next time you step into a classroom or conference room, look around. You’re sure to spot a sea of taped-over laptop cameras.⁴

Millions of consumers embrace privacy self-help strategies like Zuckerberg’s.⁵ Some communicate through encrypted messaging apps;⁶ others submit misleading information in response to marketing requests;⁷ still others shred sensitive documents.⁸ Indeed, a Pew Research Center survey reveals that

1. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, THE GUARDIAN (Jan. 10, 2010), <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>.

2. Katie Rogers, *Mark Zuckerberg Covers His Laptop Camera. You Should Consider It, Too*, N.Y. TIMES (June 23, 2016), <https://www.nytimes.com/2016/06/23/technology/personaltech/mark-zuckerberg-covers-his-laptop-camera-you-should-consider-it-too.html>.

3. See Julian Hattem, *FBI Director: Coverup Your Webcam*, THE HILL (Sept. 14, 2016), <https://thehill.com/policy/national-security/295933-fbi-director-cover-up-your-webcam>.

4. See Kurt Opsahl, *How to Protect Against Laptop Webcam Hacking*, ELEC. FRONTIER FOUND. (Apr. 29, 2013), <https://www.eff.org/deeplinks/2013/04/how-protect-against-laptop-webcam-hacking>.

5. For a definition of privacy self-help, see *infra* Part II.A. Individuals also practice self-help to protect their data from friends, family members, and the government. But those forms of self-help take different forms and serve different purposes. Thus, this Article concentrates on consumer self-help strategies.

6. See *infra* Part 0.

7. See *infra* Part II.B.2.

8. See *infra* Part 0.

almost 90% of Americans practice at least one form of privacy self-help.⁹ To put that figure in perspective, the Equifax data breach litigation—by far the largest privacy-related class action in U.S. history—covered 56% of American adults.¹⁰

The upshot is that self-help has emerged as one of the primary ways that consumers manage privacy risks. So far, however, it has attracted little attention from legal scholars.¹¹ To close that gap, this Article asks what the law should do about privacy self-help.

Courts and regulators cannot afford to ignore that question. Indeed, the same attributes that make self-help attractive to consumers also make it indispensable to legal institutions. First, self-help's *preference signaling* function tells adjudicators which types of data consumers see as sensitive.¹² By honoring consumers' self-help choices, courts and regulators empower individuals to decide what data to protect for themselves. Second, self-help's *resource conserving* function resolves low-value disputes that would otherwise consume scarce judicial and regulatory resources.¹³ In doing so, self-help enables adjudicators to concentrate their limited resources on the most serious privacy threats. Over time, harnessing those functions has become a common move across many privacy doctrines.

But privacy law's reliance on self-help may be misplaced. Too often, self-help strategies expose the data they promise to protect.¹⁴ Thanks to

9. *The State of Privacy in Post-Snowden America*, PEW RSCH. CTR. (Sept. 21, 2016), <https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/> (“Some 86% of internet users have taken steps online to remove or mask their digital footprints . . .”).

10. See Bryan Pietsch, *Factbox: Biggest U.S. Data Breach Settlements Before Equifax*, REUTERS (July 22, 2019), <https://www.reuters.com/article/us-equifax-cyber-settlement-factbox/factbox-biggest-u-s-data-breach-settlements-before-equifax-idUSKCN1UH22P>; Press Release, Off. of the Att’y Gen. for the D.C., 50 Attorneys General Secure \$600 Million from Equifax in Largest Data Breach Settlement in History (July 22, 2019), <https://oag.dc.gov/release/50-attorneys-general-secure-600-million-equifax>.

11. See generally FINN BRUNTON & HELEN NISSENBAUM, *OBFUSCATION: A USER’S GUIDE FOR PRIVACY AND PROTEST* (2016) (endorsing obfuscation, a species of self-help); Neil Richards & Woodrow Hartzog, *Privacy’s Trust Gap: A Review*, 126 YALE L.J. 1180 (2017) (identifying the downsides of obfuscation); Douglas Gary Lichtman, *How the Law Responds to Self-Help* (John M. Olin Program L. & Econ. Working Article No. 232, 2004) (discussing briefly the relationship between privacy law and self-help).

12. See, e.g., Lichtman, *supra* note 11, at 19 (explaining that self-help “distinguish[es] the bulk of normal business information from that special subset of information that warrants protection”).

13. See, e.g., Robert C. Ellickson, *Of Coase and Cattle*, 38 STAN. L. REV. 623, 686 (1986) (noting that self-help avoids the “cost[s] of carry[ing] out legal research and . . . engag[ing] in legal proceedings”).

14. See *infra* Part III (documenting the many ways that self-help backfires).

information asymmetries, data subjects struggle to distinguish successful strategies from self-defeating ones. Absent accurate intelligence about various techniques and firms' responses to them, consumers cannot escape self-help's unintended consequences, including overexposure and overreliance.

When self-help backfires, the conventional wisdom holds that courts and regulators should develop legal remedies that substitute for self-help.¹⁵ But that approach fails to appreciate the extent to which privacy law harnesses self-help's preference signaling and resource conserving functions. Displacing self-help would inadvertently disable the many doctrines that depend on those functions.

Instead, legal institutions protect consumers best when they complement—rather than replace—self-help. By supplying intelligence about self-help, this approach empowers data subjects to identify proven practices and avoid unreliable ones. By diminishing the asymmetries that distort consumers' self-help decisions, this approach strengthens the doctrines that rely on those decisions to discover data's value. And by repurposing pre-existing tools, this approach avoids the costs associated with implementing new legal rules.

More broadly, complementing self-help is appealing because it makes the most of regulators' limited resources. Thanks to self-help's popularity, even small decreases in asymmetries may translate into substantial improvements in individuals' ability to manage privacy risks. Ultimately, complementing self-help is a promising tool to promote consumer privacy that has been overlooked for too long.

To be clear, self-help is no substitute for legislative and regulatory efforts to protect consumers. Instead, self-help works best when used to address the kinds of privacy risks that more traditional tools overlook. When consumers seek to act on their own idiosyncratic preferences quickly and cheaply, self-help excels. When they face persistent and systemic risks, however, regulatory enforcement and civil litigation assume heightened importance. So, while complementing self-help represents an under-appreciated tool for advancing consumer privacy, it represents only one tool in a larger toolbox.

This Article's exploration of the promise and perils of self-help continues in Part II with a taxonomy of self-help strategies, including concealment, obfuscation, and monitoring. Marshalling evidence from a variety of disciplines, it shows that self-help has emerged as one of the main ways that consumers protect their data.

15. See, e.g., Lichtman, *supra* note 11, at 26; see also *infra* Part V.

Part III shows that certain self-help strategies produce unintended consequences, including: (1) privacy-privacy tradeoffs, (2) security-privacy tradeoffs, and (3) arms races. Information asymmetries prevent consumers from appreciating or avoiding these unforeseen harms.

Part IV highlights privacy law's surprising dependence on self-help. From the Fourth Amendment to the Federal Trade Commission's (FTC) unfairness authority, courts and regulators harness self-help to identify disputes that warrant attention and to conserve scarce judicial and regulatory resources.

Part V outlines a novel regulatory strategy. Rather than replace self-help, as the conventional wisdom suggests, courts and regulators should facilitate it. To illustrate the virtues of complementing self-help, this Part identifies three ways that legal institutions can intervene to address information asymmetries. Each intervention mobilizes pre-existing tools to arm data subjects with intelligence about self-help.

II. SELF-HELP IN PRACTICE

Twenty-five years ago, the FTC gathered scholars, technologists, and policymakers to discuss what was then the “new high-tech, global marketplace.”¹⁶ In a white paper summarizing that session, the Commission predicted that “private initiatives” such as “technology-based consumer protections and self-help opportunities” would be the key to safeguarding privacy in the twenty-first century.¹⁷

Consistent with the FTC's early optimism, almost every organization that advises consumers about privacy endorses self-help. Advocacy groups, such as the Electronic Frontier Foundation (EFF), champion self-help technologies.¹⁸ Similarly, leading newspapers—including the *New York Times*, *Wall Street Journal*, and *Washington Post*—recommend self-help strategies.¹⁹ Popular

16. FED. TRADE COMM'N., ANTICIPATING THE 21ST CENTURY: CONSUMER PROTECTION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE (1996), https://www.ftc.gov/system/files/documents/reports/anticipating-21st-century-competition-policy-new-high-tech-global-marketplace/gc_v2.pdf.

17. *Id.* at 46.

18. Opsahl, *supra* note 4; see also EPIC Online Guide to Practical Privacy Tools, ELEC. PRIV. INFO. CTR., <https://www.epic.org/privacy/tools.html> (last visited July 18, 2021).

19. See, e.g., Jonah Engel Bromwich, *Protecting Your Digital Life in 9 Easy Steps*, N.Y. TIMES (Nov. 16, 2016), <https://www.nytimes.com/2016/11/17/technology/personaltech/encryption-privacy.html>; Jennifer Valentino-DeVries, *How to Avoid the Prying Eyes*, WALL ST. J. (July 30, 2010), <https://www.wsj.com/articles/SB10001424052748703467304575383203092034876>; Hayley Tsukayama, *Must Have Gifts for Those Who Want to Protect Their Data*, WASH. POST (Nov. 16, 2017), <https://www.washingtonpost.com/news/the-switch/wp/2017/11/16/must-have-gifts-for-those-who-value-their-privacy>; Adam Levin, *8 Ways to Protect*

magazines, from *Consumer Reports* to *Wired*, follow suit.²⁰ Even public schools “teach the basics of ‘cyberhygiene,’ a kind of preventative care for the digital self.”²¹ The bottom line is that self-help has become “the dominant advice that privacy-conscious citizens encounter.”²²

This Part asks whether consumers act on that advice. After developing a definition of self-help, this Part catalogs the techniques that consumers currently practice. As quantitative and qualitative evidence attests, privacy self-help is pervasive, persistent, and varied. Though self-help is not the only way that consumers protect their personal data, it has become an important part of the picture.

A. DEFINING SELF-HELP

Before surveying consumer strategies, it is essential to clarify what counts as privacy self-help. This Article defines privacy self-help as any action that: (1) safeguards personal data, (2) without resorting to the legal system, and (3) without relying on markets.

The first element concentrates on consumer activities that safeguard personal data. While scholars dispute how to define privacy, all agree that privacy has to do with protecting personal data.²³ By analyzing various practices in terms of their effect on personal data, rather than on privacy, this Article aims to be precise about what each practice accomplishes.

The second element, which excludes legal remedies, comports with every scholarly understanding of self-help. Indeed, even the broadest definitions of self-help do not include legal remedies.²⁴ Self-help is many things, but it is not law.

The final element distinguishes between self-help and market activity.²⁵ On first glance, the line between those categories may appear blurry, or even non-

Your Privacy Online, USA TODAY (Apr. 16, 2016), <https://www.usatoday.com/story/money/personalfinance/2016/04/16/8-ways-protect-your-privacy-online/83056240>.

20. *66 Ways to Protect Your Privacy Right Now*, CONSUMER REP. (Feb. 22, 2017), <https://www.consumerreports.org/privacy/66-ways-to-protect-your-privacy-right-now>; Lil Miss Hot Mess, *infra* note 78.

21. FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* 53 (2015).

22. SARAH E. IGO, *THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA* 364–65 (2018).

23. *See, e.g.*, 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, 1835 (2011) (grappling with the various shortcomings of current legal models for defining personally identifiable information).

24. *See, e.g.*, Lichtman, *supra* note 11, at 25.

25. For a discussion of the similarities between self-help and market activity, see *infra* Part V.B.3.

existent. When a user buys an app that detects hidden cameras, for instance, is that an act of self-help, or a market transaction? To simplify matters, this Article defines market activity to encompass any practice where consumers switch between competing service providers. For example, an internet user who abandons Google in favor of DuckDuckGo (a search engine that emphasizes privacy) has engaged in market activity, not self-help.

Drawing the line here makes sense. In theory, whether competition protects privacy depends on factors, such as the structure of the market, the presence of competitors, and the non-privacy features of competing products, that are often irrelevant to self-help's success.²⁶ In practice, this definition of market activity has the advantage of ensuring that this Article does not repeat prior work, which extensively analyzes the relationship between competition and privacy while saying little about the strategies described below.²⁷

To sum up, the best way to define self-help is by clarifying what it is not. Consumers who seek to protect their data have three types of precautions to choose from: self-help, market activity, and legal remedies. Table 1, below, outlines this menu of options. Privacy self-help describes those precautions that do not involve legal remedies or market activity.

Table 1: Precautions to Protect Personal Data

| Self-Help | Market Activity | Legal Remedies |
|--|--|--|
| <i>E.g.</i> , Submitting a false name, covering laptop cameras, or shredding credit cards. | <i>E.g.</i> , Deleting an account or reducing Facebook use in favor of a competitor. | <i>E.g.</i> , Joining a class action or filing a complaint with state or federal regulators. |

B. SURVEYING SELF-HELP

Until now, scholars have paid little attention to privacy self-help. Though prior work has occasionally discussed specific strategies that fall within the definition introduced above, none surveys privacy self-help as a whole.²⁸ To

26. For an analysis of the considerations that influence self-help's effectiveness, see *infra* Part II.

27. See, e.g., Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2060 (2004) (developing a model of how privacy law should regulate the "data trade"); ERIC A. POSNER & E. GLEN WEYL, *RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY* 205–49 (2018) (proposing the creation of a market for "data labor"); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883–88 (2013) (discussing the cognitive biases that limit individuals' ability to navigate privacy in the marketplace).

28. See *supra* note 11 (collecting prior works that touch on specific self-help strategies).

fill that void, this Section marshals evidence from a variety of disciplines—from computer science to sociology—that attests to self-help’s popularity and diversity.

As the examples below illustrate, most self-help strategies share two features. First, popular techniques are invariably inexpensive; for example, common practices involve downloading free apps, covering phone cameras, and deleting files.²⁹ Such strategies enable individuals to avoid the fees that often accompany legal remedies.³⁰ Second, self-help “makes possible diverse, individuated judgments.”³¹ Put differently, self-help empowers individuals—not courts, regulators, or firms—to decide which data points warrant protection. Together, these features explain self-help’s appeal.

To organize the diverse strategies that data subjects practice, this Section introduces a three-part taxonomy: (1) *concealment strategies* limit information disclosure, (2) *obfuscation strategies* share false information, and (3) *monitoring strategies* review others’ access to personal data. Table 2, below, summarizes that taxonomy.

Table 2: Taxonomy of Self-Help Strategies

| Category | Sub-Category | Example |
|--------------------|---------------------------|---|
| Concealment | Identity data | Creating a temporary email address |
| | Sensitive data | Covering laptop and phone cameras |
| | Previously-disclosed data | Shredding sensitive documents |
| Obfuscation | Identity data | Using a fake name on social media |
| | Sensitive data | Submitting a fake address to avoid marketing requests |
| | Activity data | Generating fake social media “likes” |
| Monitoring | Personal monitoring | Using an app to detect hidden cameras |
| | Monitoring services | Hiring a reputation management service |
| | Monitoring networks | Writing app store reviews |

1. *Concealment Strategies*

According to historian Sarah Igo, “[t]he most promising contemporary avenue for achieving [privacy],” involves “carefully designed practices for hiding one’s tracks.”³² This Section describes three ways that data subjects

29. See *infra* notes 28–35.

30. See Ellickson, *supra* note 13, at 686.

31. Lichtman, *supra* note 11, at 7.

32. IGO, *supra* note 22, at 364–65.

cover their tracks: (1) concealing identifying information, (2) concealing sensitive information, and (3) retracting previously-disclosed data.

a) Concealing Identifying Information

Many practices prevent outsiders from discovering data subjects' identities. Common techniques include:

- **Creating Temporary Identifiers:** Data subjects routinely create temporary identities to safeguard their privacy.³³ About a quarter of consumers report using a temporary username or email address to conceal their identity, for instance.³⁴ Along the same lines, 18% of data subjects have employed public computers—for instance, workstations at a local library—to browse the internet without identifying themselves.³⁵ Another variant of this strategy is to pay with cash, not card. For example, *Time* instructs readers who “[d]on’t want companies knowing [about] how much booze you’re buying or other potentially embarrassing habits” to “[p]ay for things with cash.”³⁶ And some individuals even obtain disposable “burner” phones or laptops to hide their identities—although this strategy is probably limited to journalists and spies.³⁷
- **Employing Anonymization Technologies:** Some observers tout the benefits of anonymization technologies, such as “blind signatures, anonymous remailers, and encryption software.”³⁸ Scholars call these tools Privacy Enhancing Technologies (PETs).³⁹ One example of a PET is The Onion Router, or Tor.⁴⁰ By hiding individuals’ IP addresses, Tor permits them to browse the web without surveillance

33. In some cases, these practices may reflect motivations other than privacy. For example, some users may use fake email addresses to avoid spam, not to protect their anonymity. For the most part, this Article focuses on techniques for which privacy serves as the primary motivation.

34. Bruce Drake, *What Strategies Do You Use to Protect Your Online Identity?*, PEW RSCH. CTR. (Sept. 5, 2013), <https://www.pewresearch.org/fact-tank/2013/09/05/what-strategies-do-you-use-to-protect-your-online-identity>.

35. *Id.*

36. Christina DesMarais, *11 Simple Ways to Protect Your Privacy*, TIME (July 24, 2013), <https://techland.time.com/2013/07/24/11-simple-ways-to-protect-your-privacy>.

37. *See, e.g.*, Paul Sarconi, *Now’s Probably the Time to Consider One of These Burner Phones*, WIRED (Feb. 3, 2017), <https://www.wired.com/2017/02/7-great-burner-phones>.

38. IGO, *supra* note 22, at 364–65.

39. *See* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1410 (2011).

40. *See* WOODROW HARTZOG, *PRIVACY’S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* 163 (2018).

by service providers or third parties. Unlike the other self-help strategies introduced in this Part, PETs have attracted sustained attention from scholars.⁴¹ So far, however, consumers have not shown much interest in PETs. To take one example, just 2% of Americans employ anonymization software such as Tor.⁴² The most plausible explanation is that only technologically-sophisticated consumers are able to take advantage of PETs.⁴³ So, while anonymization technologies deserve attention, concentrating on PETs alone would dramatically understate the popularity of privacy self-help.

b) Concealing Sensitive Information

Instead of hiding an individual's identity, some techniques conceal sensitive categories of information. Popular practices include:

- **Constructing Physical Barriers:** In many cases, consumers install physical coverings to conceal sensitive data. The best example of this approach involves using a sticker or tape to cover laptop and smartphone cameras.⁴⁴ This strategy has won the endorsement of the FBI.⁴⁵ The popularity of this technique reflects the sensitivity of the underlying data. Webcams collect pictures of users during their most intimate moments, an obvious threat to privacy. For similar reasons, some privacy-conscious consumers seal device microphones to thwart unauthorized listeners.⁴⁶ Going even further, more sophisticated

41. See, e.g., Rubinstein, *supra* note 39, at 1417–21 (distinguishing between PETs that complement law and PETs that substitute for law). Even Brunton and Nissenbaum, who advocate for consumer obfuscation, primarily suggest technical strategies. See BRUNTON & NISSENBAUM, *supra* note 11, at 12 (“CacheCloak”); *id.* at 19 (“Tor relays”); *id.* at 21 (“Babble tapes”).

42. Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RSCH. CTR. (Mar. 16, 2015), https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

43. See, e.g., Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1673 n.383 (1999) (“Only those sophisticated enough to take advantage of public key encryption and anonymity filters may do so, with the rest of the population left defenseless due to ignorance.”).

44. See Motherboard Staff, *The Motherboard Guide to Not Getting Hacked*, MOTHERBOARD (Nov. 14, 2017), https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide.

45. Violet Blue, *The FBI Recommends You Cover Your Laptop's Webcam, for Good Reason*, ENGADGET (Sept. 23, 2016), <https://www.engadget.com/2016/09/23/the-fbi-recommends-you-cover-your-laptops-webcam-good-reasons>.

46. See, e.g., Kellen Beck, *Covering Your Webcam Isn't Enough: Here's How to Disable Your Computer's Microphone*, MASHABLE (June 22, 2016), <https://mashable.com/2016/06/22/computer-microphone-hack/>.

consumers erect screens around their property to prevent aerial surveillance, a tactic that may become more common as drones fill the skies.⁴⁷

- **Blocking Online Trackers:** An army of digital trackers follows consumers around the web, recording the sites they visit and the searches they run.⁴⁸ So it is no surprise that tracker-blocking tools have widespread appeal. Indeed, more than a third (41%) of Americans “set their browser to disable or turn off cookies.”⁴⁹ Many others (21.9%) employ apps or browser add-ins to block ads and web trackers.⁵⁰ In many cases, these technologies are free and easy to install. While these apps do not shield users’ identities completely, they limit the amount of sensitive data third-party sites collect.

c) Concealing Previously-Disclosed Information

Once consumers disclose a piece of personal data, it usually passes out of their control forever.⁵¹ That said, three techniques permit data subjects to retract data that they previously exposed but now wish to conceal:

- **Destroying Sensitive Data:** Consumer Reports recommends that readers shred any records that contain “social security number[s],” “birth date,” “credit card numbers,” “account numbers from financial institutions,” and “medical insurance numbers.”⁵² This is not a new practice. As early as 2005, 51% of Americans claimed to “always” shred financial documents, such as credit cards and bills.⁵³ Today, advocates routinely advise consumers to wipe their computers of

47. See, e.g., Carl Franzen, *The Anti-Drone Business Is About to Take Off*, POPULAR MECHANICS (May 1, 2015), <https://www.popularmechanics.com/flight/drones/a15328/droneshield-anti-drone-business/>; Heather Farmbrough, *Gatwick Fiasco Puts Anti-Drone Technology Under the Radar*, FORBES (Dec. 31, 2018), <https://www.forbes.com/sites/heatherfarmbrough/2018/12/31/gatwick-fiasco-puts-anti-drone-technology-on-the-radar/#34cea2d37708>.

48. See PASQUALE, *supra* note 21, at 33.

49. Drake, *supra* note 34.

50. *Privacy Goes Mainstream: People Take Action as Privacy Risks Increase*, DUCKDUCKGO (June 2, 2017), <https://spreadprivacy.com/privacy-settings-survey>.

51. See Solove, *supra* note 27, at 1902 (discussing the problem of unanticipated downstream uses of data).

52. CONSUMER REP., *supra* note 20.

53. ROBERT N. MAYER, AARP PUB. POL’Y INST., DEFENDING YOUR FINANCIAL PRIVACY: THE BENEFITS AND LIMITS OF SELF-HELP vi (2006), https://assets.aarp.org/rgcenter/consume/2006_06_privacy.pdf.

personal information before disposing of them.⁵⁴ In doing so, data subjects reduce the risk of identity theft—or that an unscrupulous firm will extract and resell their data.⁵⁵

- **Asking Others to Delete Data:** Most of the time, other people control our data. For example, on social media, blogs, and photo-sharing sites, friends and family members routinely share data about one another. As a result, consumers may be able to conceal data by asking others to remove it. Indeed, one study found that more than 16% of respondents “have asked someone to remove or correct information about them that was posted online.”⁵⁶
- **Harnessing Ephemeral Communications Technologies:**⁵⁷ Another way to conceal previously disclosed data relies on ephemeral communication technologies.⁵⁸ The most prominent example is Snapchat, “a photo-sharing app in which images purportedly self-destruct after being viewed.”⁵⁹ As a recent study confirms, data subjects employ Snapchat and other ephemeral software in an effort to “prevent[] the accumulation of meaningless and potentially embarrassing content.”⁶⁰ Thanks to their ability to conceal personal data, ephemeral communications technologies have become

54. Tercius Bufete, *How to Wipe a Computer Clean of Personal Data*, CONSUMER REP. (Sept. 6, 2017), <https://www.consumerreports.org/computers/how-to-wipe-a-computer-clean-of-personal-data>.

55. Recognizing that data deletion reduces risk, the FTC tells consumers how to clean their drives. See FED. TRADE COMM’N., *HOW TO PROTECT YOUR DATA BEFORE YOU GET RID OF YOUR COMPUTER* (Jan. 2020), <https://www.consumer.ftc.gov/articles/how-protect-your-data-you-get-rid-your-computer>.

56. Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RSCH. CTR. 7 (Nov. 12, 2014), <https://www.pewinternet.org/2014/11/12/public-privacy-perceptions>.

57. As we shall shortly see, not all ephemeral communication technologies live up to their promise. See *infra* Part III.A.

58. Ephemeral communications technologies can be classified as a form of self-help, as a form of market activity, or both. By switching from one app to the other, consumers encourage firms to respect privacy. As this example suggests, some techniques combine the features of market activity and self-help.

59. DANAH BOYD, *IT’S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS* 64 (2014).

60. Bin Xu, Pamara Chang, Christopher L. Welker, Natalya N. Bazarova & Dan Cosley, *Automatic Archiving Versus Default Deletion: What Snapchat Tells Us About Ephemerality in Design*, PROC. 19TH ACM CONF. ON COMPUT. SUPPORTED COOP. WORK & SOC. COMPUTING 1662, 1663 (2016).

immensely popular; in 2020, for example, Snapchat reported an average of more than 260 million daily active users.⁶¹

2. *Obfuscation Strategies*

Another way that consumers protect their data is by producing “ambiguous, confusing, or misleading information to interfere with surveillance and data collection.”⁶² This Section outlines three ways that data subjects confound observers: (1) obfuscating identifying information, (2) obfuscating sensitive information, and (3) obfuscating activity.

a) Obfuscating Identifying Information

The best example of how consumers use obfuscation to shield their identities comes from a study of teens’ Facebook use. To open an account, Facebook demands that users provide “the name you use in everyday life.”⁶³ Needless to say, this policy makes it difficult for Facebook users to conceal their identities. In response, “many teens . . . offer[] up only their first name, preferring to select a last name of a celebrity, fictional character, or friend.”⁶⁴ Indeed, about 26% of teen social media users “post fake information like a fake name . . . to help protect their privacy.”⁶⁵ This practice shields teens’ identities and retaliates against what they perceive as unnecessarily intrusive policies.⁶⁶

As today’s tech-savvy teens mature into adults, this variety of obfuscation is likely to grow even more popular. In fact, a 2013 survey revealed that 18% of Americans used a “fake name” or “untraceable username” online.⁶⁷ Since then, obfuscation techniques have become more sophisticated. For example, an app called MySudo “allows a user to create multiple email addresses and

61. Todd Spangler, *Snapchat Daily Users Pop 22% in Q4*, VARIETY (Feb. 4 2021), <https://variety.com/2021/digital/news/snapchat-q4-2020-earnings-1234901096/>.

62. BRUNTON & NISSENBAUM, *supra* note 11, at 1. Brunton and Nissenbaum were the first to use the term “obfuscation” to describe these types of techniques.

63. *Terms of Service*, FACEBOOK, <https://www.facebook.com/terms.php> (last visited Oct. 22, 2020).

64. BOYD, *supra* note 59, at 46.

65. Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith & Meredith Beaton, *Teens, Social Media, and Privacy*, PEW RSCH. CTR. (May 21, 2013), <https://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>.

66. BOYD, *supra* note 59, at 46.

67. Lee Rainie, Sara Kiesler, Ruogo Kang & Mary Madden, *Anonymity, Privacy, and Security Online*, PEW RSCH. CTR. (Sept. 5, 2013), <https://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>.

phone numbers for \$1 a month.”⁶⁸ According to MySudo’s creators, switching phone numbers and emails “eliminate[s] the ability of advertisers, scammers, and other 3rd parties [to build] a detailed profile of [users’] personal information.”⁶⁹ Similar apps have been downloaded over a million times.⁷⁰ In short, strategies that obscure users’ identities have become surprisingly common.

b) Obfuscating Sensitive Information

Consumers practice obfuscation not just to shield their identities but also to protect particularly sensitive information. For instance, *Consumer Reports* warns parents not to submit accurate data when registering “connected kids’ products” as it “essentially provides marketers and potential hackers with details about your children.”⁷¹ Instead, the magazine directs parents to “provid[e] fake information” such as inputting “Bart Simpson’s [address]—742 Evergreen Terrace.”⁷² Though quantitative research on this topic is limited, the available evidence suggests that many consumers falsify sensitive data in certain circumstances.⁷³

The appeal of obfuscating sensitive data—rather than obscuring one’s identity altogether—is that it permits consumers to pick and choose which data points to protect. As a Pew interviewee explained, “[f]or any non-essential website . . . I choose to not share my real birthday. I understand the marketing and demographic component of why they collect birthday information so I choose a fake birthday [that] is similar to my real birthday.”⁷⁴ By submitting information that is only partially misleading, savvy consumers capture disclosure’s benefits while mitigating its dangers.

68. Joel Stein, *I Tried Hiding from Silicon Valley in a Pile of Privacy Gadgets*, BLOOMBERG (Aug. 8, 2019), <https://www.bloomberg.com/news/features/2019-08-08/i-tried-hiding-from-silicon-valley-in-a-pile-of-privacy-gadgets>.

69. *MySudo*, APPLE APP STORE, <https://apps.apple.com/us/app/mysudo/id1237892621#?platform=ipad> (last visited Jan. 10, 2020).

70. *See, e.g., Burner*, GOOGLE PLAY STORE, https://play.google.com/store/apps/details?id=com.adhoclabs.burner&hl=en_US (last visited Jan. 10, 2020).

71. CONSUMER REP., *supra* note 20.

72. *Id.*

73. *See, e.g., Mayer*, *supra* note 53, at 20 (summarizing survey evidence showing that between 24 and 34 percent of respondents had “supplied false personal information” to a website).

74. *Americans Conflicted About Sharing Personal Information with Companies*, PEW RSCH. CTR. (Dec. 30, 2015), <https://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies>.

c) Obfuscating Activity

Another obfuscation strategy involves manufacturing false activity to confuse observers. For example, web searches “end up acting as lists of [consumers’] locations, names, interests, and problems.”⁷⁵ More often than not, “our identities can be inferred from these lists, and patterns in our interests can be discerned.”⁷⁶ To address that problem, researchers developed TrackMeNot, an app that “adds hundreds of false Google search queries to each legitimate one, hiding the user’s true interests in a cloud of gibberish to thwart the building of a profile of that user.”⁷⁷

Not every variant of this strategy depends on sophisticated technologies (such as TrackMeNot) to generate false activity. Consider two examples:

- **Fabricating Social Media Inputs:** As *Wired* sees it, Facebook users should “throw[] the company off [their] scent” by hiding their “real interests within a sea of not-quite-real information.”⁷⁸ To that end, the magazine urges readers to “lik[e]” random posts, “mis-tag[] photos of friends,” and “click[] all of the ads.”⁷⁹ What makes this type of activity attractive is that it promises “to confuse Facebook’s facial recognition and computer vision algorithms.”⁸⁰
- **Swapping Loyalty Cards:** Another low-tech strategy involves retail store loyalty-card programs, which collect data on consumer purchasing habits.⁸¹ In this strategy, practitioners “share[] cards . . . in *ad hoc* physical meetings, [and] with the help of mailing lists and online social networks, increasingly in large populations and over wide geographical regions.”⁸² By swapping loyalty cards, consumers create false purchasing data, confounding retailers’ efforts to analyze their behavior.

75. BRUNTON & NISSENBAUM, *supra* note 11, at 13.

76. *Id.*

77. RICHARDS & HARTZOG, *supra* note 11, at 1190.

78. Lil Miss Hot Mess, *A Drag Queen’s Guide to Protecting Your Privacy on Facebook by Breaking the Rules*, WIRED (Apr. 3, 2018), <https://www.wired.com/story/opinion-facebook-privacy>.

79. *Id.*

80. *Id.*

81. Lee Rainie & Maeve Duggan, *Scenario: Consumer Loyalty Cards and Profiling*, PEW RSCH. CTR. (Jan. 14, 2016), <https://www.pewinternet.org/2016/01/14/scenario-consumer-loyalty-cards-and-profiling>.

82. BRUNTON & NISSENBAUM, *supra* note 11, at 28–29.

3. *Monitoring Strategies*

By monitoring their data, consumers mitigate a wide range of privacy risks, from identity theft to phishing. The appeal of monitoring is that it multiplies the odds that consumers will detect privacy violations, deterring abuse by firms. At the same time, monitoring tells consumers when to engage in concealment and obfuscation, amplifying the effectiveness of other forms of self-help. This Section introduces three ways that data subjects monitor their data: (1) personal monitoring, (2) monitoring services, and (3) monitoring networks.

a) Personal Monitoring

“Carefully monitor [your] accounts for suspicious activity.”⁸³ If there is one piece of self-help advice that consumers receive more than any other, this is it. Indeed, “[t]he FTC, the California Office of Privacy Protection, the Privacy Rights Clearinghouse, Consumer Reports, and various self-help guides” all instruct data subjects to monitor their accounts.⁸⁴ Consumers put that advice into practice in the following ways:

- First, after the typical data breach, 24% of affected individuals became “more diligent” in monitoring their accounts.⁸⁵ By stepping up monitoring activity, consumers uncover misbehavior by firms—including follow-on data breaches and violations of privacy policies.
- Second, as *Consumer Reports* recognizes, readers are interested in “ferreting out which companies are sharing [their] data.”⁸⁶ To that end, the magazine suggests that subscribers “[t]ype ‘+’ before the @ symbol [in an email] and add the website’s name. Email[s] addressed to YourName+Websitename.com@gmail.com will go to the regular inbox for YourName@gmail.com. But now it will carry an extra crumb of data, and if you get spam from a company you’ve never heard of, you’ll know whom to blame.”⁸⁷

83. Paul M. Schwartz, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 949 (2007).

84. *Id.*

85. LILLIAN ABLON, PAUL HEATON, DIANA CATHERINE LAVERY & SASHA ROMANOSKY, CONSUMER ATTITUDES TOWARDS DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION 30 (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf.

86. CONSUMER REP., *supra* note 20.

87. *Id.*

- Finally, consumers download smartphone apps designed to detect hidden cameras positioned by employers, retailers, and hoteliers. For example, more than a million people have installed “Hidden Camera Detector,” an app that analyses “magnetic activity” to pinpoint concealed webcams.⁸⁸ In the wake of national news coverage of a \$100 million lawsuit alleging that a Hilton employee secretly recorded a hotel guest, camera-detection apps are likely to grow even more popular.⁸⁹
- b) Monitoring Services⁹⁰

To defend their data, individuals enlist third-party services that offer the digital equivalent of home security monitoring. Examples abound:

- First, major companies—including Experian, Equifax, and TransUnion—offer credit monitoring services. Advocacy groups routinely urge consumers to make use of these services. Privacy Rights Clearinghouse, for instance, instructs readers to “monitor your credit reports on an ongoing basis” and request “one free credit report per year from each of the three credit bureaus.”⁹¹
- Second, going beyond credit reporting, some consumers employ comprehensive monitoring services.⁹² As Frank Pasquale reports, “[c]ontracting out reputation management to a private company is a growing ‘market solution’ to the emerging traffic in data.”⁹³ Similar to a home security service, reputation managers “monitor an individual’s online reputation . . . [and] provide monthly reports to a client summarizing information about the client available online.”⁹⁴ The most expensive options offer dedicated “lawyers to review [website] terms of service . . . and reputation managers to tend to . . . online

88. See *Hidden Camera Detector*, FUTUREAPPS (July 26, 2018), <https://play.google.com/store/apps/details?id=hiddencamdetector.futureapps.com.hiddencamdetector&hl=en>.

89. See Chris Boyette & Nicole Chavez, *A Woman Is Suing Hilton for \$100M, Claiming She Was Secretly Filmed in the Shower and Blackmailed*, CNN (Dec. 5, 2018), <https://www.cnn.com/2018/12/05/us/hilton-worldwide-hotel-hidden-camera-lawsuit/index.html>.

90. These activities fall within this Article’s definition self-help because monitoring services protect privacy even if consumers never switch (or threaten to switch) to competing providers. See *supra* Part II.A (distinguishing between market activity and self-help).

91. *Top 10 Tips to Protect Your Privacy*, PRIV. RIGHTS CLEARINGHOUSE (Jan. 24, 2013), <https://www.privacyrights.org/blog/top-10-tips-protect-your-privacy>.

92. See, e.g., James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 39 (2007) (describing search engine optimization (SEO) services as a form of “self-help directed at search engines”).

93. PASQUALE, *supra* note 21, at 55.

94. Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKELEY TECH. L.J. 1103, 1145–46 (2011).

profiles.”⁹⁵ For those who can afford it, these services effectively outsource monitoring.⁹⁶

c) Monitoring Networks

The most powerful form of monitoring depends on social networks, not service providers. In practice, consumers share privacy-related feedback through the following channels:

- **App stores:** The Google, Apple, and Microsoft app stores permit consumers to share their privacy concerns in the form of reviews. At best, the prospect of negative ratings may deter developers from using personal data in ways that diverge from users’ expectations.⁹⁷ At a minimum, by complaining in app-store reviews, data subjects inform others about potential risks.⁹⁸
- **Online communities:** Several popular online communities maintain dedicated channels for users to discuss privacy risks. For instance, Reddit hosts a page for privacy-concerned users to discuss vulnerabilities in consumer-facing technologies.⁹⁹ That forum boasts more than one million members.¹⁰⁰ Other social media platforms, such as Facebook or Twitter, also enable users to exchange information about privacy threats. By disseminating intelligence about negative privacy experiences (for example, an invasive ad or message), consumers may be able to discipline firms that violate privacy norms.
- **In-person networks:** Consumers also distribute information about privacy risks through in-person networks. After having their data lost in a breach, for instance, 17% of affected users elected to “notify

95. PASQUALE, *supra* note 21, at 55.

96. See Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1383–97 (2017) (describing the burgeoning “pay-for-privacy model,” where consumers pay third parties to protect their data).

97. See, e.g., Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar & Vern Paxson, *An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps*, <https://www.icir.org/vern/papers/vpn-apps-ipc16.pdf> (identifying negative ratings that identified security vulnerabilities).

98. Admittedly, this example straddles the line between self-help and market activity. To the extent that product reviews prompt consumers to conceal or obfuscate their identity when using a particular app, those reviews qualify as a form of self-help. To the extent that reviews encourage consumers to switch from privacy-invasive to privacy-protective apps, those reviews qualify as a form of market activity.

99. See, e.g., *r/privacy*, REDDIT, <https://www.reddit.com/r/privacy> (last visited Jan. 6, 2020).

100. *Id.*

others.”¹⁰¹ Even so-called digital natives prefer to get information about privacy from their network of friends, parents, and teachers rather than online sources.¹⁰² In short, sharing negative gossip helps other consumers protect themselves, rebukes firms by damaging their reputation, and discourages future violations.

From this survey of privacy self-help, two themes emerge. First, most strategies involve low-cost ways for consumers to express their preferences. Those attributes explain much of self-help’s appeal. Second, different strategies reduce risk in different ways. Any investigation of how law should respond to self-help must account for the diversity of consumer practices. The bottom line is that self-help represents one of the primary ways that data subjects manage privacy risks. The next Part asks whether courts and regulators share consumers’ enthusiasm.

III. THE PERILS OF SELF-HELP

Too often, self-help strategies backfire. First, privacy-privacy tradeoffs mean that self-help may expose the data it promises to protect. Common techniques generate new data, enable firms to draw negative inferences, and tempt consumers to disclose more data than they would have otherwise. Second, security-privacy tradeoffs occur when consumers’ practices exacerbate security vulnerabilities, disrupting the confidentiality, integrity, and availability of data. Finally, self-help sometimes sparks wasteful arms races between firms and their customers.

To be clear, the diversity of consumer practices results in an unpredictable landscape. Although some strategies are self-defeating, others are not. So, while many techniques give rise to unintended consequences, consumers need not abandon all forms of self-help.

The problem is that data subjects struggle to predict which strategies trigger unforeseen harms. As economists warn, “consumers are often in a position of imperfect or asymmetric information regarding when their data is collected, for what purposes, and with what consequences.”¹⁰³ While the scholarly literature concentrates on how information asymmetries disrupt market transactions, those asymmetries also distort individuals’ ability to

101. ABLON ET AL., *supra* note 85, at 30.

102. See Madden, *supra* note 65 (showcasing teens’ comfort with privacy settings).

103. Alessandro Acquisti, Curtis R. Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 442 (2016).

identify successful self-help strategies.¹⁰⁴ The bottom line is that, absent accurate intelligence about which techniques backfire, data subjects cannot escape self-help's unintended consequences.

As it stands, privacy law does little to address this problem. As explained above, existing doctrines look to self-help to discern individual preferences and conserve scarce resources. At best, those doctrines do nothing to help data subjects distinguish successful techniques from self-defeating ones. At worst, by encouraging consumers to practice self-help before seeking legal remedies, privacy law may promote techniques that backfire.

This Part documents three unintended consequences of self-help: (1) privacy-privacy tradeoffs, (2) security-privacy tradeoffs, and (3) arms races between firms and consumers. Table 3 catalogs these problems.

Table 3: The Unintended Consequences of Self-Help

| Category | Sub-Category | Example |
|-----------------------------------|----------------------------|--|
| Privacy-Privacy Tradeoffs | Self-Help as Data Creation | Firms collect data about who uses self-help apps |
| | Negative Inferences | Consumers who check their credit score may betray that they are a credit risk |
| | Overreliance | Users send sensitive messages because they trust Snapchat's ephemeral communications feature |
| Security-Privacy Tradeoffs | Confidentiality | Scammers promise free credit monitoring, only to compromise user data |
| | Integrity | When consumers submit false data, security technologies malfunction |
| | Access | Breached firms cannot warn customers who conceal their contact information |
| Arms Races | Surveillance Technologies | Firms "fingerprint" devices to identify the owner |
| | Data Brokers | Firms buy concealed or obfuscated data from data brokers |

A. PRIVACY-PRIVACY TRADEOFFS

Proponents of self-help assume that consumer strategies obscure more data than they expose. But that is not always the case. This Section introduces

104. See, e.g., Solove, *supra* note 27, at 1880, 1895 (documenting the "structural problems" and "information asymmetries" that bedevil privacy decision-making); Acquisti et al., *supra* note 103, at 447 ("[T]he data subject may not know what the data holder will do with their data . . .").

three privacy-privacy tradeoffs: (1) some strategies inadvertently create new data, (2) other strategies enable observers to draw negative inferences, and (3) still other strategies tempt consumers to share more and more sensitive data than they would have otherwise.¹⁰⁵

1. *Self-Help as Data Creation*

Consumers who practice self-help risk exposing their intentions or behavior. This tradeoff affects concealment, obfuscation, and monitoring strategies alike.

First, consumers who practice concealment signal that they have something to hide. For example, the FTC warns that “sites you visit may be able to determine that you are using a VPN app.”¹⁰⁶ That information is valuable because VPN use correlates with other attributes. Indeed, lawyers, journalists, and political activists all rely on VPNs. Thus, VPN users are likely to have a job that requires them to handle sensitive information.¹⁰⁷ The upshot is that, by employing VPNs, consumers advertise that they have access to especially valuable data.

Second, obfuscation strategies suffer from a similar problem. To illustrate how obfuscation works, Professors Brunton and Nissenbaum give the example of a military aircraft that drops chaff (bundles of small metal pieces) to confuse enemy radar.¹⁰⁸ In that scenario, obfuscation distracts the enemy by generating additional targets. But dropping chaff has an obvious disadvantage: it broadcasts that at least one real target is present. In the same way, a data subject who practices obfuscation may attract extra scrutiny, either because she appears to be a security threat¹⁰⁹ or because she inadvertently discloses that she has access to information worth protecting.¹¹⁰

Finally, even monitoring strategies may inadvertently create new data. The best example involves credit monitoring services. When lenders or card issuers check a consumer’s credit score, it signals that the consumer may be about to take on new debt. “In the Heisenberg-meets-Kafka world of credit scoring,” Pasquale warns, “merely trying to figure out possible effects on one’s score can

105. Professor David Pozen coined the term “privacy-privacy tradeoffs.” See David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 222 (2016).

106. Andrea Arias, *Virtual Private Networks (VPN) Apps*, FED. TRADE COMM’N. (Feb. 22, 2018), <https://www.consumer.ftc.gov/blog/2018/02/shopping-vpn-app-read>.

107. See BRUNTON & NISSENBAUM, *supra* note 11, at 89–90 (discussing the motivations for political protesters and journalists to adopt obfuscation techniques).

108. *Id.* at 8.

109. See *infra* Part III.B.

110. See *infra* Part II.B.2.

reduce it.”¹¹¹ Indeed, one individual who repeatedly checked the ownership of his mortgage note “reported . . . a 40-point hit on his credit score after his inquiry.”¹¹²

Unfortunately, many consumers do not appreciate this tradeoff. Economists often emphasize “how invisible [data] collection is to the data subject.”¹¹³ And, as the FTC’s warning about VPNs illustrates, data collection about self-help is no more visible than data collection about any other activity.¹¹⁴ Without intelligence about which self-help techniques generate personal data, consumers may not be able to distinguish effective practices from self-defeating ones.

2. *Negative Inferences*

Even when self-help shields personal data from direct observation, firms may be able to draw inferences based on the absence of data. Game theorists recognize that when a data subject declines to disclose information, that choice reveals something about the subject.¹¹⁵ For example, suppose that you decide not to share certain data on online financial forms. In response, banks may infer that you are hiding undesirable characteristics, such as unpaid debts. Because observers can draw inferences based on the absence of information, concealing one piece of data often exposes other, more sensitive data.

What scholars call “unraveling effects” exacerbate this problem.¹¹⁶ As Scott Peppet explains, “[a]t first, those with positive private information . . . will disclose to seek discounts and economic benefit.”¹¹⁷ Next, “even those with the worst private information . . . may realize that they have little choice but to disclose to avoid the stigma of keeping information secret.”¹¹⁸ Ultimately, “privacy may unravel as those who refuse to disclose are assumed to be withholding negative information and therefore stigmatized and penalized.”¹¹⁹

111. PASQUALE, *supra* note 21, at 24.

112. *Id.*

113. Alessandro Acquisti, *Privacy and Market Failures: Three Reasons for Concern, and Three Reasons for Hope*, 10 J. TELECOMM. & HIGH TECH. L. 227, 229 (2012).

114. *See* FED. TRADE COMM’N., *supra* note 106.

115. *See* DOUGLAS G. BAIRD, ROBERT H. GERTNER & RANDAL C. PICKER, *GAME THEORY AND THE LAW* 89–95 (1998).

116. Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U.L. REV. 1153, 1156 (2011). The concept of “unraveling” in repeated games is not unique to privacy, but it derives from game theory. *See* BAIRD, *supra* note 115, at 89–95; Ian Ayres, *Playing Games with the Law*, 42 STAN. L. REV. 1291, 1306 (1990).

117. Peppet, *supra* note 116, at 1176.

118. *Id.*

119. *Id.* at 1156.

Thanks to unraveling effects, firms' ability to draw inferences depends on the volume of personal data they possess. The more consumers who disclose personal data, the more likely that firms will be able to draw negative inferences about those who choose to conceal their data. But data subjects typically lack information about the size and quality of firms' data sets.¹²⁰ For that reason, consumers struggle to predict whether or to what extent self-help will permit firms to draw negative inferences.

3. *Overreliance*

In some cases, the availability of self-help encourages consumers to expose personal data that they would not have otherwise. Generally, "higher perceived control over information publication increased [data] subjects' propensity to disclose sensitive information."¹²¹ For example, consider Snapchat, an app that promises to protect users' communications.¹²² But Snapchat did not always live up to that promise. At one point, users could capture screenshots or use third-party apps to save each other's messages.¹²³ If every Snapchat user had realized that recipients could preserve their communications, many would have sent fewer messages—or none at all.

As this example suggests, overreliance is only an issue when practitioners overestimate the effectiveness of a particular strategy. In Snapchat's case, technically-proficient users were able to detect the problem years before the FTC intervened.¹²⁴ The more difficult it is for consumers to assess the effectiveness of a given strategy, the greater the risk of overreliance.

The result is that consumers cannot assume that self-help obscures more data than it reveals. Many self-help techniques invite privacy-privacy tradeoffs, exposing more data—or more sensitive data—than practitioners anticipate.

B. SECURITY-PRIVACY TRADEOFFS

Every day, cybercriminals attempt to access consumer data. Every day, corporate security experts try to stop them.¹²⁵ More specifically, corporate

120. See Solove, *supra* note 27, at 1889.

121. Acquisti, *supra* note 113, at 230.

122. Complaint at 8, *In re* Snapchat, Inc., FTC File No. 1323078, No. C-450 (Dec. 23, 2014), <https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf>.

123. *Id.* at 3.

124. See Kashmir Hill, *Snapchats Don't Just Disappear: Forensics Firm Has Pulled Dozens of Supposedly-Deleted Photos from Android Phones*, FORBES (May 9, 2013), <https://www.forbes.com/sites/kashmirhill/2013/05/09/snapchats-dont-disappear/#2801d2192bdd>.

125. See Kim S. Nash, *For Many Companies, a Good Cyber Chief Is Hard to Find*, WALL ST. J. (May 15, 2017), <https://www.wsj.com/articles/for-many-companies-a-good-cyber-chief-is-hard-to-find-1494849600> ("About 65% of large U.S. companies now have a CISO position . . .").

security teams safeguard the confidentiality, integrity, and availability of customer data—what experts call the “CIA triad.”¹²⁶ *Confidentiality* prevents unauthorized access to data, *integrity* verifies that data is accurate, and *availability* ensures that authorized users can access their data.¹²⁷

Too often, privacy self-help disrupts the CIA triad. Borrowing from David Pozen, the previous Section used the term “privacy-privacy tradeoffs” to describe situations where “preserving privacy along a certain axis may entail compromising privacy along another axis.”¹²⁸ This Section introduces a parallel concept, security-privacy tradeoffs, to refer to practices that bolster privacy at the expense of security. By compromising confidentiality, integrity, and availability, some self-help strategies frustrate firms’ attempts to protect personal data.

1. Confidentiality

Champions of self-help often endorse technology-dependent strategies, such as hidden camera apps and VPNs.¹²⁹ But trusting third-party technologies has a downside: it opens the door for malicious attackers. In many cases, harmful programs masquerade as self-help-style software.¹³⁰ But once a consumer clicks a link or downloads a file, the application steals their data. The FTC has identified two examples of this security-privacy tradeoff:

- First, take Scareware, a type of malware that “falsely claim[s] that scans ha[ve] detected viruses, spyware, and illegal pornography on consumers’ computers.”¹³¹ The FTC explains that these programs “trick consumers into thinking their computers [a]re infected with malicious software” and then “s[ell] [the consumers] software to ‘fix’ the[] non-existent problem.”¹³² In this way, self-help provides an opportunity for cybercriminals to trick consumers into downloading applications that compromise their data.

126. Kristen E. Eichensehr, *Giving up on Cybersecurity*, 64 UCLA L. REV. DISCOURSE 320, 324 (2016).

127. See BRUCE SCHNEIER, *CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD* 78 (2018) (explaining that the CIA triad aims to prevent outsiders from “steal[ing] a copy of [data], modify[ing] it, or delet[ing] it.”).

128. Pozen, *supra* note 105, at 222.

129. See *supra* Part 0.

130. See *How to Spot, Avoid and Report Tech Support Scams*, FED. TRADE COMM’N. (Feb. 2019), <https://www.consumer.ftc.gov/articles/0263-free-security-scams> [<https://perma.cc/QYV9-8NY9>].

131. *Operator of Deceptive "Scareware" Scheme Will Pay More than \$8 Million to Settle FTC Charges*, FED. TRADE COMM’N. (Jan. 27, 2011), <https://www.ftc.gov/news-events/press-releases/2011/01/operator-deceptive-scareware-scheme-will-pay-more-8-million>.

132. *Id.*

- Second, experts warn that some VPNs exacerbate security vulnerabilities.¹³³ “[W]hen you use a VPN app,” the FTC says, “you are giving the app permission to intercept all of your internet traffic.”¹³⁴ As security researchers caution, some “VPN apps . . . expose users to serious privacy and security vulnerabilities, such as use of insecure VPN tunneling protocols.”¹³⁵

Information asymmetries prevent consumers from discerning these unintended consequences. According to one survey, for instance, “only a marginal number of . . . users” recognize that VPN apps may reveal personal data.¹³⁶ If consumers cannot distinguish applications that protect personal data from ones that expose it, self-help may do more harm than good. At a minimum, by encouraging data subjects to take privacy into their own hands, self-help opens the door for Scareware and unreliable VPNs.

2. Integrity

Self-help also threatens the second component of the CIA triad: data integrity. To see why, it is helpful to have a basic understanding of anomaly-based intrusion detection systems (IDS).¹³⁷ Firms rely on these systems to “detect intrusion attempts by comparing current account activities against a ‘normal activity profile.’”¹³⁸ “When the IDS detects abnormal activity (outside normal boundaries as identified in the baseline),” cybersecurity expert Darril Gibson explains, “it gives an alert indicating a potential attack.”¹³⁹ In doing so, these systems safeguard customer data from hackers and other threats.

The problem with practices that ask users to act “outside normal boundaries” is that they risk triggering false IDS alerts.¹⁴⁰ Obfuscation strategies may be the worst offender. By definition, submitting large volumes of false searches or clicks will be “abnormal” compared with consumers’

133. Andrea Arias, *Shopping for a VPN app? Read this.*, FED. TRADE COMM’N. (Feb. 22, 2018), <https://www.consumer.ftc.gov/blog/2018/02/shopping-vpn-app-read>.

134. *Id.*

135. Ikram et al., *supra* note 97, at 1.

136. *Id.* at 6 (“Only less than 1% of the negative reviews relate to security and privacy concerns, including the use of abusive or dubious permission requests and fraudulent activity . . .”).

137. See, e.g., Arnt Brox, *Signature-Based or Anomaly-Based Intrusion Detection: The Practice and Pitfalls*, SC MEDIA (May 1, 2002), <https://www.scmagazine.com/home/security-news/features/signature-based-or-anomaly-based-intrusion-detection-the-practice-and-pitfalls>.

138. Michael Lee, Sean Park, Tae Kim, David Lee, Aaron Schapiro & Tamer Francis, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 853 (1999).

139. Darril Gibson, COMP TIA SECURITY+ GET CERTIFIED GET AHEAD 181 (2014).

140. *Id.*

baseline. If a user starts submitting random searches in Vietnamese, for example, an IDS may not be able to tell whether the sudden behavior change is the product of an obfuscation strategy or a hacker's intrusion. In other words, IDS technologies may interpret obfuscation as a sign that a malicious attacker has gained access to customer accounts. The sad reality is that, because obfuscation produces false positives, it confuses the security systems designed to protect consumer data.

Few data subjects appreciate this tradeoff. As Pew Research complains, "many [Americans] struggle with more technical cybersecurity concepts."¹⁴¹ If consumers do not understand security basics, they cannot identify which self-help techniques are likely to interfere with companies' security efforts.

3. *Availability*

In addition to threatening confidentiality and integrity, self-help also endangers the availability of data, the final component of the CIA triad. Consider three examples:

- First, imagine that you run a data processing firm. Your security team discovers that a data breach has occurred. In turn, your lawyers recommend that you notify affected users about the breach.¹⁴² To do so, you need access to valid names, email addresses, or phone numbers for each user. On reviewing the relevant records, however, you discover that many customers have concealed their contact information. As this example illustrates, strategies that shield consumers from unwanted communications from firms may inadvertently prevent them from receiving essential notifications.
- Second, Facebook assumes that accounts with fake names involve "malicious intent to violate [their] policies."¹⁴³ Accordingly, the social media giant promises to "remove" the accounts of users who practice obfuscation.¹⁴⁴

141. Aaron Smith, *What the Public Knows About Cybersecurity*, PEW RSCH. CTR. (Mar. 22, 2017), <https://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity>.

142. See CAL. CIV. CODE § 1798.29 (West 2006).

143. *Fake Accounts*, FACEBOOK, <https://transparency.fb.com/data/community-standards-enforcement/fake-accounts/facebook/> (last visited Aug. 15, 2021).

144. See *Community Standards Enforcement Preliminary Report*, FACEBOOK, <https://transparency.facebook.com/community-standards-enforcement#fake-accounts> (last visited Oct. 30, 2020) (reporting that Facebook disabled 583 million fake accounts in the first quarter of 2018 alone).

- Third, suppose that you practice obfuscation by submitting false names, email addresses, and security questions. The simple fact that it can be more difficult to remember many different lies than it is to recall a single truth may mean that consumers who practice obfuscation ultimately struggle to authenticate their identities and regain access to their accounts.

Again, data subjects do not always take this tradeoff into account when deciding whether to engage in self-help. Indeed, a recent survey found that “a significant share of online adults are simply not sure of the correct answer on a number of cybersecurity knowledge questions.”¹⁴⁵ Without an understanding of security basics, consumers may struggle to predict which self-help strategies will cause them to lose access to their data.

To be clear, not every strategy undermines security. Indeed, some low-tech strategies shield both privacy and security. Covering laptop cameras, for example, protects data from both firms and hackers. The trouble is that, if consumers do not appreciate security tradeoffs, they cannot tell which strategies endanger data security.

C. ARMS RACES

Consumers do not have a monopoly on self-help. To the contrary, “self-help can initiate wasteful ‘arms races’ between providers and consumers.”¹⁴⁶ These arms races are distinct from the privacy-privacy tradeoffs introduced above. Section III.A argued that some self-help strategies are self-defeating because they create new data, permit negative inferences, and induce over-reliance. During an arms race, by contrast, firms counter consumer self-help with strategies of their own.

The best-documented example of an arms race between consumers and firms involves copyright protection.¹⁴⁷ At the start of the race, consumers share content in violation of copyright restrictions through tools like LimeWire. Then creators respond by “develop[ing] more secure, tamper-resistant management systems.”¹⁴⁸ At the end of the day, consumers and content creators would be better off cooperating.¹⁴⁹ But because they are trapped in a

145. Smith, *supra* note 141.

146. Lee Kovarsky, *A Technological Theory of the Arms Race*, 81 IND. L.J. 917, 918 (2006).

147. Dan L. Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121, 167 (1999).

148. *Id.*

149. See Stephen J. Majeski, *Arms Races as Iterated Prisoner's Dilemma Games*, 7 MATHEMATICAL SOC. SCI. 253, 253 (1984) (“[I]ndividually rational behavior does not lead to a cooperative, group preferred outcome.”).

prisoner's dilemma, rational decisions on each side lead to "wasteful investment[s]" in "hacking and protection technology."¹⁵⁰

Privacy arms races follow a similar pattern. When consumers practice self-help, the economics of personal data encourage firms to respond with strategies of their own. As *The Economist* observes, personal data is the new oil.¹⁵¹ It follows that when self-help strategies reduce the quantity of data available, firms have a powerful incentive to circumvent those strategies.¹⁵² To do so, firms either: (1) install surveillance technologies, or (2) buy personal data from brokers.

1. *Surveillance Technologies*

The most obvious way to circumvent self-help is through surveillance technologies. Imagine, for instance, that customers start refusing to fill out forms on a company's website. In response, that company may decide to deploy trackers that follow the customer around the internet. Today, such counterattacks by firms are commonplace.¹⁵³

For the most part, firms prefer surveillance technologies that consumers cannot detect. Take "fingerprinting," a technique that "uniquely identif[ies] computers" by reference to details such as "clock setting, different fonts, [and] different software."¹⁵⁴ As the *Wall Street Journal* reports, "fingerprinting is largely invisible" to consumers.¹⁵⁵ Indeed, "[i]t's tough even for sophisticated Web surfers to tell if their gear is being fingerprinted."¹⁵⁶

For another example, consider a recent study that attempted to identify all of the ways that Facebook gathers personal data. The researchers found that the social media giant consolidates data from the Facebook Messenger app, phone contact lists, and data uploaded to user accounts for "two-factor

150. Burk, *supra* note 147, at 167.

151. *Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data*, *ECONOMIST* (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

152. See Imanol Arrieta Ibarra, Leonard Goff, Diego Jimenez Hernandez, Jaron Lanier & E. Glen Weyl, *Should We Treat Data as Labour? Moving Beyond "Free"*, *AEA ARTICLES & PROC.* 2 (May 2018) (stressing the importance of accurate data for machine learning); POSNER & WEYL, *supra* note 27, at 221 (observing that insufficient data can preclude the development of working algorithms).

153. See PASQUALE, *supra* note 21, at 53.

154. Julia Angwin & Jennifer Valentino-DeVries, *Race Is on to 'Fingerprint' Phones, PCs*, *WALL ST. J.* (Nov. 30, 2010), <https://www.wsj.com/articles/SB10001424052748704679204575646704100959546>.

155. *Id.*

156. *Id.*

authentication.”¹⁵⁷ Even data “obtained without a user’s knowledge, such as by some other user syncing their phone contacts . . . is used for PII-based advertising.”¹⁵⁸

As these examples indicate, firms identify creative ways to collect personal data without alerting consumers.¹⁵⁹ The appeal of these invisible data collection technologies is obvious: consumers cannot respond to a counterattack they cannot detect in the first place.

2. *Data Brokers*

Not all firms have access to the same surveillance technologies as Facebook. But they all have access to data brokers.¹⁶⁰ These entities “collect and maintain data on hundreds of millions of consumers.”¹⁶¹ Thanks to brokers, “[h]uge databases of usernames, credit card numbers, and social security numbers already exist online.”¹⁶² By selling access to those databases, brokers offer a cost-effective way to circumvent self-help.

Indeed, data brokers thrive because they enable counterattacking firms to avoid detection. To that end, many brokers refuse “to identify the specific sources of their data or the [firms] who purchase it.”¹⁶³ In doing so, brokers make it “impossible for a consumer to determine the originator of a particular data element.”¹⁶⁴ To understand which self-help strategies fall victim to data brokers, data subjects need information about the types of data that brokers sell and who they sell it to. Otherwise, consumers cannot predict when brokers will enable firms to circumvent self-help.¹⁶⁵

Of course, not every self-help strategy sparks an arms race. While data brokers and surveillance technologies are powerful, their reach does not

157. Giridhari Venkatadri, Elena Lucherini, Piotr Sapiezynski & Alan Mislove, *Investigating Sources of PII Used in Facebook’s Targeted Advertising*, SCIENDO: PROC. ON PRIV. ENHANCING TECHS. 227 (2018).

158. *Id.* at 240. PII stands for personally-identifiable information.

159. *See, e.g.*, Acquisti, *supra* note 113, at 229 (commenting on “how invisible such collection is to the data subject”).

160. *See* Steven H. Hazel, *Personal Data as Property*, 70 SYRACUSE L. REV. (forthcoming 2020).

161. S. COMM. ON COM., SCI., & TRANSP., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES i (Dec. 18, 2013) [hereinafter A REVIEW OF THE DATA BROKER INDUSTRY].

162. PASQUALE, *supra* note 21, at 53.

163. *Id.* at iii.

164. FED. TRADE COMM’N., DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 14 (May 2014).

165. *See id.* at iii.

extend to every person and every type of data.¹⁶⁶ But consumers struggle to distinguish strategies that are vulnerable to arms races from those that are not. Firms exacerbate this problem by engaging in invisible arms races. Unaware of hidden counterattacks, data subjects fail to adopt alternative strategies that could better protect their data. At the same time, consumers continue to waste resources implementing unsuccessful strategies, harming social welfare.

Taken together, privacy-privacy tradeoffs, security-privacy tradeoffs, and arms races threaten self-help's appeal. In an ideal world, consumers would avoid strategies that backfire and prioritize ones that succeed. But information asymmetries limit consumers' ability to discern which strategies produce unforeseen harms. So, absent accurate intelligence about various strategies and firms' responses, consumers cannot escape self-help's unintended consequences.

IV. HOW PRIVACY LAW HARNESSSES SELF-HELP

What, if anything, should privacy law do about self-help? To answer that question, it is first necessary to understand the relationship between existing privacy doctrines and self-help. For the most part, the same attributes that make self-help appealing to consumers also make it useful to legal institutions. First, self-help's *preference signaling* function helps adjudicators discern which types of data consumers view as sensitive.¹⁶⁷ Second, self-help's *resource conserving* function resolves low-value disputes that would otherwise consume scarce judicial and regulatory resources.¹⁶⁸ Over time, privacy law has come to depend on these functions.

To illustrate how existing doctrines harness self-help, this Part introduces five disparate examples: the Fourth Amendment, the Electronic Communications Privacy Act (ECPA), Article III standing, privacy torts, and state data breach notification laws. Each doctrine depends on self-help to identify disputes that warrant attention and to husband judicial and regulatory resources.

166. See DAVID BRIN, *THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM?* 218 (1998) (positing that firms are less likely to circumvent unpopular strategies).

167. See Lichtman, *supra* note 11, at 19 (explaining that self-help “distinguish[es] the bulk of normal business information from that special subset of information that warrants protection”).

168. See, e.g., Ellickson, *supra* note 13, at 686 (noting that self-help avoids the “cost[s] of carry[ing] out legal research and . . . engag[ing] in legal proceedings”).

A. THE FOURTH AMENDMENT

The Supreme Court's "reasonable expectation of privacy test" may be the best-known rule in privacy law. In *Katz v. United States*, the Court held that whether government activity counts as a Fourth Amendment search hinges on the searched citizen's "reasonable expectation of privacy."¹⁶⁹ In a concurrence, Justice Harlan set out the two-pronged test that courts continue to apply today. Under Harlan's test, the Fourth Amendment applies when: (1) the defendant exhibits a "subjective" expectation of privacy, and (2) that expectation is "one that society is prepared to recognize as 'reasonable.'"¹⁷⁰

In elaborating the first prong, Justice Harlan warned that, "objects, activities, or statements that [a citizen] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."¹⁷¹ This "knowing exposure" requirement clarifies that citizens who do not engage in reasonable self-help measures forfeit the Fourth Amendment's protection.¹⁷² In *Katz*, for example, it was essential that the defendant had "shut[] the door" to the phone booth that the government surveilled.¹⁷³ Closing the door signaled that the defendant regarded his conversations within that booth as private. The same logic explains why citizens who fail to engage in reasonable forms of self-help—such as installing fencing,¹⁷⁴ affixing roof panels,¹⁷⁵ or securely disposing of garbage¹⁷⁶—forfeit constitutional protection. Ultimately, *Katz*'s "knowing exposure" test looks at self-help to divine whether a given data point deserves protection.

B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

Similar reasoning guides courts' analyses of the Electronic Communications Privacy Act (ECPA). That statute prescribes criminal and civil penalties for those who intercept electronic, oral, and wire communications.¹⁷⁷

169. *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

170. *Id.* at 361.

171. *Id.*

172. *Id.*

173. *Id.*

174. *See United States v. Dunn*, 480 U.S. 294, 303 (1987) (holding that respondent's interior fencing did not indicate a reasonable expectation of privacy).

175. *See Florida v. Riley*, 488 U.S. 445, 450 (1989) (declining to recognize a reasonable expectation of privacy in part because the defendant left "the sides and roof of his greenhouse . . . partially open").

176. *See California v. Greenwood*, 486 U.S. 35, 40–41 (1988) ("[S]ociety would not accept as reasonable respondents' claim to an expectation of privacy in trash left for collection in an area accessible to the public . . .").

177. 18 U.S.C. § 2511.

In defining ECPA's scope, Congress imported *Katz*'s "knowing exposure" test. By its terms, the Act applies when plaintiffs "[exhibit] an expectation that such communication is not subject to interception under circumstances justifying such expectation."¹⁷⁸ To decide whether this requirement is satisfied, courts look to self-help. Indeed, ECPA only protects plaintiffs who take "common-sense precautions . . . to preserve their expectation of privacy," as the Fifth Circuit has observed.¹⁷⁹

Consider *Huff v. Spaw*, where the chair of a corporate board pocket-dialed a colleague.¹⁸⁰ Though the colleague quickly realized that the chair had called her by accident, she stayed on the line for over an hour, listening in on an embarrassing conversation between the chair, the chair's spouse, and a third-party. In denying the chair's ECPA claim, the Sixth Circuit faulted him for failing to engage in any of the "simple and well-known measures [to] prevent pocket-dials."¹⁸¹ For example, the plaintiff could have "lock[ed] the phone, set[] up a passcode, [or] us[ed] one of many downloadable applications that prevent pocket-dial calls."¹⁸² The court even cited a magazine article that recommended self-help-style apps that reduce the risk of pocket dials.¹⁸³

Huff illustrates how courts harness self-help's preference signaling function to reduce the cost of discerning data's value. Because the plaintiff failed to take self-help measures that would have protected his information, the Sixth Circuit was able to infer that his privacy interest was minimal.¹⁸⁴ At the same time, by requiring that plaintiffs practice "simple and well-known measures" before resorting to ECPA, the *Huff* court conserved judicial resources.¹⁸⁵ The bottom line is that, without ECPA's self-help requirement, courts would need to wrestle with many more low-value cases than they do today.

C. ARTICLE III STANDING IN DATA BREACH CASES

To satisfy Article III's standing requirement, plaintiffs must show an injury-in-fact that is "concrete and particularized" and "actual or imminent."¹⁸⁶ In recent years, courts have struggled to apply this standard to data breach

178. 18 U.S.C. § 2510(2) (defining an "oral communication").

179. *Kee v. City of Rowlett, Texas*, 247 F.3d 206, 216–17 (5th Cir. 2001).

180. *See Huff v. Spaw*, 794 F.3d 543, 545–46 (6th Cir. 2015).

181. *Id.* at 552. The Sixth Circuit determined that the Chairman's wife, Bertha Huff, may have had a viable ECPA claim. *See id.* at 554.

182. *Id.* at 552.

183. *See id.* (citing Will Verduzco, *Prevent Unwanted Butt Dialing with Smart Pocket Guard*, XDADEVELOPERS (Apr. 15, 2014), <https://www.xdadevelopers.com/android/prevent-unwanted-butt-dialing-with-smart-pocket-guard>).

184. *See id.*

185. *Id.*

186. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016).

claims. During a breach, hackers gain access to consumer data but do not inevitably use that data in ways that harm consumers. Thus, whether a given data breach threatens “imminent” injury is not always apparent.¹⁸⁷

Although not dispositive on its own, self-help assists courts in determining whether a data breach creates sufficient risk to satisfy Article III standing. In *Remijas v. Neiman Marcus*, for instance, the Seventh Circuit confronted a breach of a major retailer’s customer records.¹⁸⁸ The retailer confirmed that a breach had occurred, acknowledged the risk, and even recommended that customers implement credit monitoring.¹⁸⁹ In those circumstances, the court reasoned that “[a]n affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring.”¹⁹⁰ Because many consumers did engage in self-help, and because those decisions were reasonable, the Seventh Circuit determined that the risk of harm was sufficient to support standing under Article III.¹⁹¹

As *Neiman Marcus* illustrates, consumers’ self-help decisions provide a shortcut to gauge the threat posed by a given data breach. If few members of a putative class practice credit monitoring or other self-help strategies, it is unlikely that they see the breach as a substantial threat. But if many class members embrace those strategies, then the “risk of harm” may be “sufficiently substantial” to establish standing.¹⁹² In this way, self-help enables courts to focus their resources on the data breaches that pose the greatest risk.¹⁹³

D. PRIVACY TORTS

Thanks to Samuel Warren and Louis Brandeis’s famous law review article, *The Right to Privacy*, most states recognize privacy-related torts.¹⁹⁴ To adjudicate

187. *Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017).

188. *See Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. 2015).

189. *Id.* (“It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection . . .”).

190. *Id.*

191. The Seventh Circuit is not alone in harnessing self-help to decide whether plaintiffs in data breach cases have demonstrated standing. *See, e.g., Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App’x 384, 388 (6th Cir. 2016).

192. *Id.*

193. An analysis of the risk posed by a data breach remains relevant even after the Supreme Court’s decision in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021). *TransUnion* observes that a “mere risk of future harm” does not establish Article III standing when a plaintiff seeks damages. *Id.* at 2211. But the decision makes clear that “a person exposed to a risk of future harm may pursue forward-looking, injunctive relief.” *Id.* at 2210.

194. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 219 (1890).

those claims, courts usually must decide whether a given piece of information is sufficiently “private” to merit protection.¹⁹⁵ Though courts examine many factors in this analysis, the outcome often turns on whether the plaintiff engaged in self-help to conceal, obscure, or monitor her data.

Take the public disclosure of private facts tort.¹⁹⁶ To prevail on such a claim, a plaintiff must show that the defendant gave “publicity to matters concerning the private, as distinguished from the public, life of the individual.”¹⁹⁷ This element “seeks to differentiate between those facts whose disclosure promotes intimacy and those whose disclosure does not.”¹⁹⁸ Generally, courts sort private facts from public ones by asking whether the plaintiff engaged in self-help. Consistent with that approach, courts recognize “no liability for giving further publicity to what the plaintiff himself leaves open to the public eye.”¹⁹⁹

For example, in *Gill v. Hearst Publishing Co.*, a couple objected to the dissemination of a photograph that showed them “seated in an affectionate pose” in a restaurant.²⁰⁰ But the couple did nothing to block the camera’s view or to discourage the photographer.²⁰¹ The court therefore rejected the couple’s claim, emphasizing that the picture “was not surreptitiously snapped . . . but rather was taken of plaintiffs in a pose voluntarily assumed in a public market place.”²⁰² By displaying their affection where other people could observe them, the plaintiffs signaled that their information was not sensitive enough to warrant judicial protection.

Just like the doctrines described above, privacy torts harness self-help. To distinguish private and public information, courts must make difficult decisions about what data deserves protection. Self-help offers a way out. By honoring consumers’ self-help choices, courts allow individuals to decide which data to protect for themselves.

195. Restatement (Second) of Torts § 652D (1977).

196. The application of the intrusion upon seclusion tort also turns on whether the plaintiff practices self-help. *See id.* § 652B (“The defendant is subject to liability under the rule stated in this Section only when he has . . . invaded a private seclusion that the plaintiff *has thrown about* his person or affairs.”) (emphasis added).

197. Restatement (Second) of Torts § 652D.

198. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 930 (2005).

199. Restatement (Second) of Torts § 652D.

200. *Gill v. Hearst Pub. Co.*, 40 Cal. 2d 224, 226 (1953).

201. *Id.* at 230–31.

202. *Id.*

E. DATA BREACH NOTIFICATION STATUTES

Today, a significant number of U.S. states have enacted legislation requiring firms to notify affected consumers about data breaches.²⁰³ In general, these statutes specify which incidents require notification and prescribe the content of those communications. Such statutes serve many purposes, from “impos[ing] a reputational sanction on breached entities” to creating a private right of action for consumers.²⁰⁴

But the primary goal of notification laws is to encourage consumers to practice self-help. Consider California’s statute, which has emerged as a model for other states.²⁰⁵ As the state’s Office of Privacy Protection explains, mandatory notifications are “intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves.”²⁰⁶ To that end, California requires that notification letters specifically tell consumers about “What [They] Can Do” to mitigate risks.²⁰⁷ The premise is that, if notification letters prompt consumers to practice self-help, there will be less demand for the involvement of state or federal regulators. Like the doctrines introduced above, data breach notification statutes use self-help to preserve regulators’ resources.

In sum, privacy law depends on self-help to solve two of its most pressing problems. First, self-help’s preference signaling function helps adjudicators discern whether a given piece of data deserves protection. By honoring consumers’ self-help choices, courts and regulators empower individuals to decide what data to protect for themselves.²⁰⁸ Second, self-help’s resource conserving function filters out the many low-value privacy disputes that might otherwise overwhelm the legal system. In doing so, self-help enables adjudicators to concentrate their limited resources on the most serious privacy threats.

In the future, self-help’s preference signaling and resource conserving functions may grow even more essential. According to one estimate, modern

203. Taryn Elliott, *Standing a Chance: Does Spokeo Preclude Claims Alleging the Violation of Certain State Data Breach Laws?*, 49 SETON HALL L. REV. 233, 242 (2018) (observing that all fifty states have passed data breach notification statutes).

204. Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 917, 925 (2007).

205. See CAL. CIV. CODE § 1798.29 (West Supp. 2006).

206. CAL. DEP’T OF CONSUMER AFF., OFF. OF PRIV. PROT., RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 5 (2007).

207. CAL. CIV. CODE §§ 1798.29, 1798.80, 1798.82 (as amended, 2016).

208. See Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 929 n.25 (2005) (observing that individuals are generally “in a better position than government officials to make decisions about sharing personal information”).

society “create[s] as much information in two days . . . as we did from the dawn of man through 2003.”²⁰⁹ The more data consumers create, the more often that adjudicators will need to decide what to protect. For that reason, reliance on self-help is likely to remain a common feature of privacy doctrines. Turning from the descriptive to the normative, the remainder of this Article asks how the law should respond to privacy self-help.

V. THE CASE FOR COMPLEMENTING SELF-HELP

Courts and regulators can respond to self-help in one of two ways. The first option is to develop legal remedies that substitute for self-help. The second option is to complement self-help by addressing the information asymmetries that undermine it.

The conventional wisdom endorses the first approach. In this view, privacy law and self-help are substitutes. As Douglas Lichtman maintains, “privacy law might be explained simply on th[e] notion that the law obviates the need for costly self-help measures.”²¹⁰ Along the same lines, Woodrow Hartzog and Neil Richards posit that “first-best privacy [sh]ould be promoted through law rather than self-help.”²¹¹ Channeling Annie Oakley, the traditional view is that anything self-help can do, law can do better.

But the conventional wisdom misses the mark. As an initial matter, it is far from obvious that legislators could devise legal remedies that are sufficiently low-cost such that they present consumers with a meaningful alternative to self-help. For the most part, self-help and legal remedies specialize in different types of privacy risks: self-help enables consumers to vindicate their preferences quickly and cheaply, while litigation addresses persistent, systemic risks. Even in the best of circumstances, bringing a privacy-related lawsuit costs money, takes many months or even years, and yields uncertain results. By contrast, most of the self-help techniques surveyed in Part II promise instant results at almost no expense. Under those circumstances, it is difficult to see how even the most potent privacy legislation could convince consumers to abandon self-help.

And even if policymakers could achieve that improbable result, it would produce unexpected—and unwelcome—consequences. As Part IV explained, privacy law has come to rely on self-help’s preference signaling and resource

209. MG Siegler, *Eric Schmidt: Every 2 Days We Create as Much Information as We Did up to 2003*, TECHCRUNCH (Aug. 4, 2010).

210. Lichtman, *supra* note 11, at 26.

211. RICHARDS & HARTZOG, *supra* note 11, at 1207.

conserving functions.²¹² Displacing self-help would disable the many doctrines that depend on those functions.

Compared with the conventional wisdom, complementing self-help has many virtues.²¹³ By arming data subjects with intelligence about self-help, this approach empowers them to select successful strategies and sidestep self-defeating ones. By diminishing the asymmetries that distort consumers' self-help decisions, this approach supports the doctrines that rely on those decisions to discover data's value. And by repurposing familiar tools, this approach avoids the costs associated with formulating new legal rules.

Above all, complementing self-help makes the most of regulators' limited resources. Thanks to self-help's popularity, even small decreases in information asymmetries may translate into big improvements in consumers' ability to manage privacy risks. That means that complementing self-help is a promising tool to promote privacy that has been overlooked for too long.

A. HOW LAW CAN COMPLEMENT SELF-HELP

Just as law depends on self-help, self-help also depends on law. This Section identifies three ways that courts and regulators can reduce the information asymmetries that undermine self-help: (1) revisiting generally applicable laws, (2) extracting intelligence about self-help from data processing firms, and (3) disrupting invisible arms races that perpetuate asymmetries.

1. *Revisiting Generally Applicable Laws That Exacerbate Asymmetries*

On a regular basis, privacy and security researchers shed light on self-help.²¹⁴ For example, computer scientists have called attention to the security-privacy tradeoffs associated with VPNs.²¹⁵ In a similar vein, experts recently revealed that firms track users' devices in an attempt to circumvent concealment strategies.²¹⁶ By identifying the strategies and circumstances that

212. See, e.g., Ellickson, *supra* note 13, at 686 (explaining that self-help avoids the “cost[s] of] carry[ing] out legal research and . . . engag[ing] in legal proceedings”).

213. Two decades ago, David Brin identified a “class of solutions to privacy issues, whose approach is not to close down information flows, but rather to compensate by opening them wider.” BRIN, *supra* note 166, at 81. Complementing self-help falls into that class: by supplying consumers with intelligence about self-help, legal institutions help them protect their personal data.

214. See, e.g., *The Computer Fraud and Abuse Act Hampers Security Research*, ELEC. FRONTIER FOUND. (Feb. 13, 2013), <https://www.eff.org/document/cfaa-and-security-researchers> (“Computer scientists are studying how advertisers and other companies track consumers’ activities online . . .”); Ikram et al., *supra* note 97, at 2 (finding that certain VPN apps amplify rather than resolve security vulnerabilities).

215. See Ikram et al., *supra* note 97, at 2.

216. See, e.g., ELEC. FRONTIER FOUND., *supra* note 214.

produce unforeseen harms, this sort of research reduces the information asymmetries that plague self-help.

But many generally applicable laws discourage this vital research.²¹⁷ Commercial contracts prevent data brokers from sharing their clients' secrets, non-disclosure agreements stop employees at data processing firms from speaking with researchers, and trade secret law shields details about new surveillance technologies.²¹⁸ Though these generally applicable laws serve important functions, they have the unfortunate side effect of exacerbating the information asymmetries that plague self-help.

The Computer Fraud and Abuse Act (CFAA) may be the worst offender. That Act establishes criminal and civil penalties for individuals that access a computer “without authorization” or who “exceed[] authorized access.”²¹⁹ In interpreting the CFAA, “most courts . . . have held that a conscious violation of a website’s terms of service/use will render the access unauthorized and/or cause it to exceed authorization.”²²⁰ In practice, terms of service usually forbid activities—such as creating fake accounts or engaging in automated monitoring—that scientists use to gather intelligence about self-help.²²¹ So, by criminalizing terms of service violations, the CFAA inadvertently discourages research that sheds light on self-help’s unintended consequences.

This is not a theoretical concern. Consider *Sandvig v. Sessions*, where scientists petitioned the court to issue a declaratory injunction shielding them from CFAA liability.²²² In *Sandvig*, the plaintiffs’ proposed project would have studied employment discrimination, not privacy self-help. But the scientists planned to use the same methods as privacy and security researchers, such as

217. See, e.g., A. Michael Froomkin, “PETs Must Be on a Leash”: How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology, 74 OHIO ST. L.J. 1, 2 (2013) (“[L]egal rules and corporate policies . . . block . . . privacy self-help in the form of Privacy Enhancing Technologies . . .”).

218. See SCHNEIER, *supra* note 127, at 41 (2018) (noting that the Digital Millennium Copyright Act “includes a prohibition against security research”).

219. 18 U.S.C. § 1030(a)(2).

220. *United States v. Drew*, 259 F.R.D. 449, 460 (C.D. Cal. 2009).

221. For example, Facebook demands that users “[p]rovide accurate information about yourself” and “[c]reate only one account.” See *Terms of Service*, FACEBOOK, <https://www.facebook.com/terms.php> (last revised Oct. 22, 2020). Similar provisions are commonplace. See, e.g., *Terms and Conditions*, THE ATLANTIC, <https://www.theatlantic.com/terms-and-conditions> (last updated Oct. 5, 2020) (warning users not to “[f]orge headers or otherwise intentionally disguis[e] the origin of any content or communication”); *Apple Website Terms of Use*, APPLE, <https://www.apple.com/legal/internet-services/terms/site.html> (last updated Nov. 20, 2009) (stating that users should not “manipulate identifiers in order to disguise the origin of any message or transmittal you send to Apple”).

222. *Sandvig v. Sessions*, 315 F. Supp. 3d 1, 14 (D.D.C. 2018).

“misrepresenting their identities to target websites” and “[s]craping data.”²²³ In the end, the District Court concluded that “it would be credible [for researchers] to fear a future [CFAA] prosecution” for engaging in those activities.²²⁴

There is no doubt that the CFAA discourages research on privacy self-help. For example, take the “Persons You May Know (PYMK) Inspector,” an app that helps users monitor how Facebook collects data and circumvents self-help.²²⁵ As the app’s developers explain, “Facebook won’t discuss the input it uses, [so] the alternative is to study the output it produces: to track your friend suggestions and see how they change from day to day.”²²⁶

Soon after the researchers released the app, “a Facebook spokesperson . . . told [them] that the tool violated Facebook’s terms of service.”²²⁷ Threatened with liability under the CFAA, the researchers reluctantly agreed to modify the tool.²²⁸ As this example illustrates, the Act chills research that could provide consumers with intelligence about self-help strategies and firms’ responses to them.

But while the CFAA currently amplifies information asymmetries, it need not do so. Fortunately, legislative action is not necessary to fix the problem. Indeed, it would be easy for courts and regulators to ensure that the CFAA does not chill privacy and security research. First, courts should read the CFAA not to criminalize violations of a website’s terms of service.²²⁹ Rather, liability should only attach to defendants who undertake code-based hacking, a

223. *Id.* at 15–16.

224. *Id.* at 19.

225. Kashmir Hill & Surya Mattu, *Keep Track of Who Facebook Thinks You Know with This Nifty Tool*, GIZMODO (Jan. 10, 2018), <https://gizmodo.com/keep-track-of-who-facebook-thinks-you-know-with-this-ni-1819422352>.

226. *Id.*

227. Kashmir Hill & Surya Mattu, *Facebook Wanted Us to Kill This Investigative Tool*, GIZMODO (Aug. 7, 2018), <https://gizmodo.com/facebook-wanted-us-to-kill-this-investigative-tool-1826620111>.

228. *Id.* (“Facebook is happy to have users hand over lots of data about themselves, but doesn’t like it when the data flows in the other direction.”).

229. How far the Supreme Court’s recent interpretation of the CFAA goes towards accomplishing this result remains unclear. *See generally Van Buren v. United States*, 141 S. Ct. 1648 (2021). Though the Court held that liability under the CFAA’s “exceeds authorization” provision implicates “a gates-up-or-down inquiry,” *id.* at 1658, it declined to decide whether that “inquiry turns only on technological . . . limitations on access, or instead also looks to limits contained in contracts or [website] policies,” *id.* at 1659 n.8. So, whether a researcher’s violation of a website’s terms of service would trigger CFAA liability is a question the appellate courts must resolve. *See infra* note 230 (collecting cases).

conclusion that the Second and Fourth Circuits already embrace.²³⁰ Second, prosecutors should promise not to bring charges against privacy and security researchers. The Department of Justice (DOJ) has already taken a step in this direction. In 2014, it released an “Intake and Charging Policy for Computer Crime Matters” that instructs prosecutors to consider “[t]he extent to which the activity was in furtherance of a larger criminal endeavor or posed a risk of bodily harm.”²³¹

Of course, creating a safe harbor in the CFAA is just one example of how revisiting generally applicable laws can complement self-help. Other doctrines, including the Digital Millennium Copyright Act, are also interpreted and enforced in ways that discourage privacy and security research.²³² By establishing safe harbors in such laws, policymakers can promote research that provides consumers with vital information about self-help.

2. *Extracting Intelligence from Data Processing Firms*

Another way for courts and regulators to reduce information asymmetries is by encouraging data processing firms—the institutions that know the most about self-help—to share that intelligence with consumers. This approach does not require policymakers to develop new statutes or promulgate new rules. Instead, regulators already have access to an array of familiar tools that are designed to encourage disclosure.

Most important, the FTC has statutory authority to monitor data processing firms.²³³ In establishing the Commission, Congress gave it “[the] power . . . to gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices,

230. *See, e.g.*, *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204, 206 (4th Cir. 2012). In these cases, the Second and Fourth Circuits held that the CFAA does not hinge on a website’s terms of use but rather on whether an individual violates technical barriers—that is, whether the defendant engages in hacking. By contrast, the First, Fifth, Seventh, and Eleventh Circuits concluded that whether defendants act without authorization or exceed authorized access depends in part on the policies and terms of the computer owner. *See* *EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577, 583 (1st Cir. 2001); *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010); *Int’l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418, 421 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258, 1263–64 (11th Cir. 2010).

231. OFF. OF THE ATT’Y GEN., MEMORANDUM TO THE UNITED STATES ATTORNEYS AND ASSISTANT ATTORNEY GENERALS FOR THE CRIMINAL AND NATIONAL SECURITY DIVISIONS 2 (2014), <https://www.justice.gov/criminal-ccips/file/904941/download>.

232. *See, e.g.*, SCHNEIER, *supra* note 127, at 41 (explaining how the Digital Millennium Copyright Act discourages security research and proposing improvements).

233. *See* Thomas Pahl, *Your Cop on the Privacy Beat*, FED. TRADE COMM’N. (Apr. 20, 2017), <https://www.ftc.gov/news-events/blogs/business-blog/2017/04/your-cop-privacy-beat>.

and management of any...corporation engaged in...commerce.”²³⁴ Also, Congress “empowered [the FTC] to make public the information obtained, except trade secrets and names of customers.”²³⁵ As scholars of consumer protection law observe, agency monitoring powers of this kind are ideally suited to address “information asymmetries.”²³⁶

But the Commission rarely employs its monitoring authority to protect consumer privacy.²³⁷ Instead, the FTC “decides whether to open an investigation by relying mostly on publicly available information and consumer complaints.”²³⁸ That information comes from “industry conferences, online consumer complaints, or litigators watching television in search of deceptive ads.”²³⁹ So, despite the agency’s extensive monitoring powers, FTC investigators may suffer from the same information asymmetries as the consumers they protect.

By activating its dormant monitoring authority, the FTC could level the informational playing field. For example, the agency might decide to investigate the secretive data broker industry.²⁴⁰ Through its monitoring authority, the Commission could identify “specific sources of [broker] data” and “the [firms] who purchase it.”²⁴¹ At best, publishing that information would discourage firms from dealing with brokers in the first place. At a minimum, consumers would know not to rely on self-help when transacting with firms that buy data from brokers.

This is not to say that the FTC needs to limit its monitoring activities to data brokers. The Commission could also gather intelligence about firms’ security measures, educating users about which self-help strategies disrupt those systems.²⁴² Or the FTC could study the circumstances in which missing data enables firms to draw negative inferences.²⁴³ The bottom line is that by engaging its pre-existing monitoring powers, the FTC can equip data subjects with intelligence about which self-help strategies succeed and when.

234. 15 U.S.C. § 46(a) (West 2006); *see also* Kenneth Culp Davis, *The Administrative Power of Investigation*, 56 YALE L.J. 1111, 1118 (1947) (describing the history of this provision).

235. *Id.*; *see also* 15 U.S.C. § 46(f).

236. Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 COLUM. L. REV. 369, 404 (2019).

237. Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. PA. L. REV. 1311, 1379 (2015) (“[U]nlike financial regulators, the FTC does not exercise these powers.”).

238. *Id.* at 1380.

239. Van Loo, *supra* note 236, at 411.

240. *See supra* Part III.C.2.

241. *See* A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 161, at iii.

242. *See supra* Part III.B.2.

243. *See supra* Part III.A.2.

3. *Disrupting Invisible Arms Races*

When data subjects practice self-help, firms respond in kind, sparking arms races. Unsurprisingly, firms prefer to undermine self-help with strategies—such as data brokers and surveillance technologies—that consumers cannot detect.²⁴⁴ Unaware of these hidden counterattacks, data subjects fail to adopt alternative strategies that could better protect their data.

Though regulators cannot prevent all arms races, they can ensure that when firms counterattack, they do so openly. To disrupt invisible arms races, the FTC has a powerful tool at its disposal: the authority to block unfair practices.²⁴⁵ The agency’s three-part unfairness test requires: (1) a “substantial injury to consumers,” (2) “which is not reasonably avoidable by consumers themselves,” and (3) is “not outweighed by countervailing benefits.”²⁴⁶ As it turns out, most invisible arms races satisfy all three of those elements.

First, counterattacks that undo self-help generally cause “substantial injury” to data subjects.²⁴⁷ The reason is that consumers usually use self-help to safeguard data they consider sensitive.²⁴⁸ Second, when consumers cannot detect firms’ responses to self-help, the harm is—almost by definition—not “reasonably avoidable.”²⁴⁹ After all, the purpose of hidden surveillance technologies and undisclosed data broker agreements is to prevent consumers from avoiding them.²⁵⁰ Finally, counterattacks typically lack countervailing consumer benefits. At a minimum, this element requires firms to explain why invisible arms races benefit consumers—and many practices will be difficult to justify.

To see how unfairness claims can complement self-help, consider the Commission’s complaint against DesignerWare, “a company that licensed software to rent-to-own stores to help them track and recover rented computers.”²⁵¹ Unbeknownst to users, DesignerWare’s software, called PC

244. See *supra* Part III.C.

245. Because more than forty states have passed consumer protection laws modeled on the FTC Act, state regulators have the ability to bring unfairness claims as well. See John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 638–39 (2018) (“Some but not all of these state laws are interpreted according to the FTC’s unfairness standard.”).

246. 15 U.S.C. § 45(n).

247. *Id.*

248. As noted above, some legal doctrines adopt that presumption explicitly. See, e.g., *supra* Part IV.A–B.

249. See 15 U.S.C. § 45(n).

250. See *supra* Part III.C.

251. Press Release, Fed. Trade Comm’n., FTC Halts Computer Spying (Sept. 25, 2012), <https://www.ftc.gov/news-events/press-releases/2012/09/ftc-halts-computer-spying>.

Rental Agent, “log[ged] key strokes, capture[d] screen shots and t[ook] photographs using a computer’s webcam.”²⁵² By hiding these surveillance tools, DesignerWare ensured that consumers could not engage in self-help to defeat them. As the FTC cautioned, “[c]onsumers cannot reasonably avoid [the harms stemming from data collection] because PC Rental Agent is *invisible* to them.”²⁵³ Soon after the FTC filed suit, DesignerWare agreed to stop selling its tracking software.²⁵⁴

Despite the benefits of shutting down invisible arms races, however, the FTC rarely does so.²⁵⁵ One explanation is that the agency’s unfairness authority may rest on a shaky foundation. For years, critics have complained that unfairness authority is so broad that regulated entities lack notice about what conduct counts as unfair.²⁵⁶ Validating those concerns, the Eleventh Circuit recently held that FTC remedial orders in unfairness cases must direct defendants “to stop committing a specific act or practice.”²⁵⁷

But when unfairness claims target invisible arms races, concerns about specificity and notice lose much of their force. Regarding specificity, when a firm employs a surveillance technology to circumvent self-help, the natural response is for the FTC to forbid that “specific . . . practice.”²⁵⁸ As for notice, after DesignerWare, firms are on notice that invisible arms races may give rise to unfairness claims.²⁵⁹ So, even if some unfairness claims raise concerns about notice and specificity, claims that target invisible arms races do not. By

252. *Id.*

253. Complaint at 19, *In re DesignerWare, LLC*, FTC File No. 123151, No. C-4390, 5 (Apr. 15, 2013), <https://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter> (emphasis added).

254. *See FTC Halts Computer Spying, supra* note 251 (outlining the terms of the proposed settlement orders).

255. Apart from *DesignerWare*, my research only uncovered two cases that targeted invisible arms races. *See* Complaint, *In re Lenovo (USA) Inc.*, FTC File No. 1523134, No. C-4636, 6 (Dec. 20, 2017), https://www.ftc.gov/system/files/documents/cases/1523134_c4636_lenovo_united_states_complaint.pdf (explaining that pre-installed software blocked access to VPNs); Complaint for Permanent Injunction and Other Equitable and Monetary Relief, Fed. Trade. Comm’n. v. Vizio, Inc., No. 2:17-cv-00758, 2017 WL 7000553, (D.N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.

256. Most criticism of the FTC’s unfairness authority has arisen in data security cases. *See, e.g.,* Fed. Trade. Comm’n. v. Wyndham Worldwide Corp., 799 F.3d 236, 255 (3d Cir. 2016) (rejecting the defendant’s claim that they lacked fair notice that their conduct violated 18 U.S.C. § 45).

257. *LabMD, Inc. v. Fed. Trade Comm’n.*, 894 F.3d 1221, 1236 (11th Cir. 2018).

258. *Id.* at 1233.

259. *See* Complaint, *supra* note 253, at 5 (emphasis added).

stepping up unfairness enforcement, regulators can help data subjects figure out which strategies fall victim to arms races and which do not.

This Article began by asking how the law should respond to self-help. The conventional wisdom, which favors displacing self-help, fails to recognize that many privacy doctrines depend on it. Complementing self-help holds more promise. By disseminating intelligence about self-help, courts and regulators increase the odds that consumers will embrace proven practices while avoiding unreliable ones.

B. COMPLICATIONS

This Section acknowledges three objections that complicate the case for complementing self-help. The first objection contends that facilitating self-help is not feasible, while the second and third posit that it is not desirable. Though none of these objections are fatal, they underscore that self-help is an imperfect tool for advancing consumer privacy. Even if courts and regulators eliminate information asymmetries, they cannot transform self-help into a cure for every privacy problem. So, while policymakers should devote more resources to supporting self-help than they do today, legal remedies and market activity will remain essential tools for protecting personal data.

1. *The Gap Between Information and Action*

The interventions introduced above assume that consumers will act on the intelligence that regulators and researchers disseminate. But disclosures do not always influence consumer behavior. As quantitative research attests, data subjects rarely review or understand privacy policies.²⁶⁰ Should consumers ignore intelligence about self-help, they may continue to practice strategies that backfire.²⁶¹

260. See, e.g., Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S92 (2016) (“[D]ifferences in [privacy] policy language that are quite salient to lawyers are essentially irrelevant to consumers.”); Aleccia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL’Y FOR INFO. SOC’Y 543, 565 (2009) (“We estimate that reading privacy policies carries costs in time of approximately 201 hours a year, worth about \$ 3,534 annually per American Internet user.”).

261. A related problem is that educated, wealthy consumers may be better equipped to implement effective self-help strategies. See generally Mary Madden, *Privacy, Security, and Digital Inequality: How Technology Experiences and Resources Vary by Socioeconomic Status, Race, and Ethnicity*, DATA & SOC’Y. (Sept. 27, 2017), https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf. That raises a real concern that the availability of self-help may exacerbate distributional differences in access to privacy. At the same, other privacy protection mechanisms—such as class-action lawsuits—may well suffer from similar problems, so the broader distributional effects of complementing self-help remain far from clear.

Of course, empirical evidence is the only way to conclusively determine the extent to which data subjects act on intelligence about self-help.²⁶² That said, consumers are far more likely to read and apply intelligence about self-help than other privacy information. Privacy policies, after all, supply information that is unimportant to most readers. By contrast, data subjects only practice self-help when they believe that a given piece of data is worth protecting. For this reason, consumers may be particularly likely to pay attention to—and act on—intelligence about which self-help strategies succeed and which fail.

2. *The Social Costs of Self-Help*

It is no secret that some self-help strategies inflict social costs.²⁶³ To take one example, Facebook users who create “many false and implausible life events on their profiles . . . might confuse networked connections.”²⁶⁴ In turn, that may lead to lost friendships, or, at a minimum, wasted time. Worse still, self-help may deprive firms of data that ultimately benefits consumers.

And, while complementing self-help does not raise social costs itself, it does not reduce them either. That is because individuals generally overlook social costs when making decisions.²⁶⁵ So, even if consumers enjoy perfect information about such costs, they may still decide to pursue strategies that inflict them. Thus, if the magnitude of social costs is large, self-help may cause serious problems that the interventions introduced above do nothing to solve.

Two considerations mitigate this concern. First, many popular self-help strategies do not impose social costs. For instance, while taping over laptop cameras creates some private costs—no one wants sticky camera lenses—it has no obvious social costs. To the contrary, if installing camera covers inspires other consumers to do the same, it may generate social benefits. Second, while some unusual techniques inflict substantial social costs, existing legal doctrines generally deter those techniques. If, for example, an individual hacks into a

262. One possibility is that behavioral biases will prevent consumers from acting. *See, e.g.*, Solove, *supra* note 27, at 1883–88 (examining how cognitive biases interfere with individuals’ privacy decision-making); Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1096 (2009) (“[R]esearch in behavioral economics and behavioral decision making [sic] provides ample evidence that consumers are unable to conceive of all possible outcomes and risks of data disclosures.”).

263. *See* RICHARDS & HARTZOG, *supra* note 11, at 1207–08 (raising the issue of social costs in the context of obfuscation strategies.).

264. *Id.*

265. *See, e.g.*, Carl J. Dahlman, *The Problem of Externality*, 22 J.L. & ECON. 141, 141 (1979) (“[W]e say that when an externality is present there is a divergence between private and social cost.”).

firm's network as a form of self-help, that firm can bring a civil claim or even press criminal charges.²⁶⁶

So, for the most part, self-help strategies either do not impose substantial social costs or are adequately deterred by existing criminal and civil penalties. To the extent that some strategies inflict social costs without triggering liability, new legal remedies may be necessary to discourage those strategies or mitigate their effects. Thus, while courts and regulators generally should facilitate self-help, it may sometimes be necessary to displace particularly wasteful strategies.

3. *The Market Alternative to Self-Help*

In a competitive market, consumers need not resort to self-help to protect their interests. Instead, they can exit, taking their business—and their data—to another firm. In this way, market activity replicates self-help's ability to express individual preferences and to do so cheaply. At the same time, market activity encourages firms to compete by enhancing privacy features.²⁶⁷ So, when exit is an option, self-help may be a second-best solution.

As a result, it is tempting to conclude that the law should ignore self-help and instead encourage consumers to manage privacy risks through market activity. But data subjects routinely encounter problems that exit cannot solve. For one thing, some platforms may be so ubiquitous that consumers cannot disentangle themselves without incurring substantial costs.²⁶⁸ For another thing, markets do not always permit consumers to address granular privacy risks. Recall, for instance, the Pew interviewee who revealed most personal data but concealed her birthday.²⁶⁹ Even firms that tout dashboards that

266. For example, in one case, a group of individuals allegedly created thousands of fake accounts on LinkedIn, degrading the value of that social network. In response, LinkedIn brought a variety of federal and state law claims, including some under the CFAA. *See* Complaint, LinkedIn Corp. v Does, No. 5:15-cv-04463, (N.D. Cal. Aug. 8, 2016), <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2261&context=historical>.

267. *See* Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1009 (2013) (“Within a neoclassical economic framework, the relationship between Internet privacy and competition is direct and positive.”).

268. *See, e.g.*, Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 81 (2019).

269. *See* *Americans Conflicted About Sharing Personal Information with Companies*, PEW RSCH. CTR (Dec. 30, 2015), <https://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies>.

purportedly give users control over their data²⁷⁰ rarely permit such granular choices.²⁷¹

Because markets cannot solve every problem that consumers encounter, self-help is likely to remain a popular tool to protect privacy. So, while courts and regulators should facilitate competitive markets, they must also complement self-help.

VI. CONCLUSION

Today, privacy self-help is endorsed by journalists, championed by advocates, and embraced by consumers. Too often, however, self-help exposes the data that it promises to protect. In an ideal world, consumers would avoid strategies that backfire and adopt ones that succeed. But information asymmetries prevent data subjects from discovering which strategies and circumstances produce unforeseen harms.

While displacing self-help falls short because it disrupts existing doctrines, complementing self-help succeeds because it works with them. This approach preserves individuals' ability to decide what data deserves protection, strengthens the many doctrines that depend on self-help, and harnesses familiar regulatory tools. Ultimately, complementing self-help promises to transform a popular but unreliable practice into a potent weapon in the hands of millions of consumers.

270. For example, Google states that its privacy settings permit users to control how data is used across Google. *Privacy Controls*, GOOGLE, <https://safety.google/privacy/privacy-controls> (last visited Nov. 25, 2020); *see also* Paddy Underwood, *Privacy Checkup Is Now Rolling Out*, FACEBOOK (Sept. 4, 2014), <https://newsroom.fb.com/news/2014/09/privacy-checkup-is-now-rolling-out>.

271. *See* Fred Stutzman, Ralph Gross & Alessandro Acquisti, *The Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIV. & CONFIDENTIALITY 7, 23 (2012) (“Choosing Facebook privacy settings to correctly match one’s preferences can be difficult.”).

ANTITRUST IN THE CONSUMER PLATFORM ECONOMY: HOW APPLE HAS ABUSED ITS MOBILE PLATFORM DOMINANCE

Shili Shao[†]

ABSTRACT

Apple's iOS smartphone platform wields de facto monopoly power thanks to its dominant revenue share and Apple's sticky product ecosystem. Apple has abused this power to tie the distribution of digital goods on iOS to its proprietary in-app purchase payment system to impose a 30% tax and extract supracompetitive profits. Moreover, Apple has blocked rivals and favored its own apps using its control of the App Store, distorting competition both on the iOS platform and between smartphone platforms. Courts today are increasingly hostile to lawsuits against dominant firm behavior, however, creating doctrinal obstacles that impede antitrust enforcement against tech platforms such as Apple.

This Note makes the antitrust case against Apple and explores why features of consumer tech platforms Apple represents demand a reform of the current antitrust regime.

DOI: <https://doi.org/10.15779/Z380K26C09>

© 2021 Shili Shao.

[†] Yale Law School, J.D. I am immensely grateful to Babu Kotapati, Simon Mutungi, Melissa Newham, Jeff Schroeder, and Melody Wang for research collaboration and inspiration. I am also indebted to Fiona Scott Morton and Florian Ederer for helpful comments and encouragement, and to Austin Frerick and Yale's Thurman Arnold Project for research support. I further thank Doni Bloomfield, Kenneth Khoo, and George Priest for thoughtful feedback. The views expressed in this Note are solely my own and do not represent the views of any institution with which I have been affiliated.

TABLE OF CONTENTS

| | | |
|--------------|--|------------|
| I. | INTRODUCTION | 355 |
| II. | THE MYTHICAL BENIGN MONOPOLIST | 360 |
| III. | THE CONSUMER PLATFORM ECONOMY | 364 |
| | A. CONSUMERS AS KEY ECONOMIC ACTORS | 365 |
| | B. SMALL BUSINESSES AND APP DEVELOPERS | 366 |
| | C. ECOSYSTEM LOCK-INS | 368 |
| | D. MULTILAYERED DYNAMIC NETWORKS | 369 |
| IV. | APPLE'S DOMINANCE: DE FACTO MONOPOLY | 371 |
| | A. MARKET SHARE | 372 |
| | B. BARRIERS TO ENTRY | 373 |
| | C. DIRECT EVIDENCE | 374 |
| V. | TYING: FORCING THE APPLE TAX | 378 |
| | A. ESTABLISHING THE IAP TIE | 379 |
| | 1. <i>Separability</i> | 380 |
| | 2. <i>Forceful Conditioning</i> | 380 |
| | B. CONSUMER HARM: TAXING THE APP ECONOMY | 381 |
| VI. | MONOPOLIZATION: FORTIFYING THE WALLED GARDEN. | 384 |
| | A. BLOCKING COMPETITORS, RESTRICTING RIVALS, AND SELF- PREFERENCING | 385 |
| | 1. <i>Block Competitors</i> | 385 |
| | 2. <i>Restrict Rivals</i> | 387 |
| | 3. <i>Self-Preferencing</i> | 388 |
| | B. RAISE RIVALS' COSTS: EXCLUSIONARY AND COLLUSIVE EFFECTS .. | 388 |
| | C. PROLONG THE PLATFORM MONOPOLY | 389 |
| VII. | HOLLOW EFFICIENCIES AND LESS RESTRICTIVE ALTERNATIVES | 393 |
| | A. IAP TIE | 394 |
| | B. IMPAIRING RIVALS | 396 |
| VIII. | ANTITRUST FOR THE 21ST CENTURY | 398 |
| | A. RECONSIDER LEVERAGING | 398 |
| | B. RATIONALIZE THE REFUSAL TO DEAL DOCTRINE | 400 |
| | C. RECALIBRATE ENFORCEMENT: CLASS CERTIFICATION AND PRIVATE- PUBLIC DIVISION OF LABOR | 404 |
| | 1. <i>Private Class Actions</i> | 404 |
| | 2. <i>Public Enforcement</i> | 409 |

IX. CONCLUSION 411

I. INTRODUCTION

In March 2019, Spotify filed an antitrust complaint with the European Commission alleging that Apple's various tactics to impair competitors on Apple devices such as the iPhone violated European competition law.¹ Spotify argued that Apple gave its Apple Music streaming service unfair advantages over rivals including Spotify through Apple's control of its App Store. Apple's rules "purposely limit[ed] choice and stifle[ed] innovation at the expense of the user experience—essentially acting as both a player and referee to deliberately disadvantage other app developers," wrote Spotify CEO Daniel Ek.²

Spotify's complaint against Apple came at a time when big technology companies were also under increasing scrutiny in the United States due to their growing dominance. Just days before Spotify announced its legal battle against Apple, Senator Elizabeth Warren published her ambitious plan to break up U.S. tech giants.³ Later in 2019, both the Department of Justice (DOJ) and the Federal Trade Commission (FTC)—America's two federal agencies enforcing antitrust law—as well as the House Antitrust Subcommittee, launched broad investigations into potential anticompetitive practices of Google, Apple, Facebook, and Amazon (collectively, "GAFA").⁴ Earlier, the Supreme Court

1. See Daniel Ek, *Consumers and Innovators Win on a Level Playing Field*, SPOTIFY (Mar. 13, 2019), <https://newsroom.spotify.com/2019-03-13/consumers-and-innovators-win-on-a-level-playing-field>.

2. *Id.*

3. Elizabeth Warren, *Here's How We Can Break Up Big Tech*, MEDIUM (Mar. 8, 2019), <https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c>.

4. See Brent Kendall, *Justice Department to Open Broad, New Antitrust Review of Big Tech Companies*, WALL ST. J. (July 23, 2019), <https://www.wsj.com/articles/justice-department-to-open-broad-new-antitrust-review-of-big-tech-companies-11563914235>; Tony Romm, *House Lawmakers Ask Apple, Amazon, Facebook and Google to Turn Over Trove of Records in Antitrust Probe*, WASH. POST (Sept. 13, 2019), <https://www.washingtonpost.com/technology/2019/09/13/house-lawmakers-ask-apple-amazon-facebook-google-turn-over-trove-records-antitrust-probe>. The House Antitrust Subcommittee released the results of its investigation on GAFA in October 2020 (after the writing of this Note's substantially completed manuscript), relying in part on this Note's sister paper on Apple. See MAJORITY STAFF OF H. SUBCOMM. ON ANTITRUST, COMMERCIAL & ADMIN. L. OF THE H. COMM. ON THE JUDICIARY, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 369, <https://int.nyt.com/data/documenttools/house-antitrust-report-on-big-tech/b2ec22cf340e1af1/full.pdf> (citing Babu Kotapati, Simon Mutungi, Melissa Newham, Jeff Schroeder, Shili Shao & Melody Wang, *The Antitrust Case Against Apple*, YALE UNIV., THURMOND ARNOLD PROJECT, DIGIT. PLATFORM

approved a group of iPhone consumers' legal standing to sue Apple for its anticompetitive practices.⁵ Epic Games, distributor of one of the most popular applications ("apps") on iPhone, filed a lawsuit challenging Apple's allegedly anticompetitive practices in August 2020; similar actions by other third-party developers against Apple are also going through the courts.⁶

Apple represents a particularly interesting example of tech platform dominance. While all of GAFAM command enormous size and profitability, Apple controls a critical gateway to the modern digital economy on which all the other tech giants sit: the iPhone mobile platform. Although Google's Android provides limited competition, the iPhone mobile platform's dominant position in capturing mobile revenue means that most of the mobile economy's innovations happen first, if not exclusively, on the iPhone.⁷ Apple's control over the App Store, where all iPhone apps such as Spotify are distributed, thus gives it extraordinary power to dictate the terms of the digital economy.

To say Apple's iPhone has been a blockbuster success is a gross understatement. Apple has sold more than 1.4 billion iPhones since it introduced the device in 2007, reaching about a quarter of the world population.⁸ According to long-time Apple analyst Ben Thompson, the iPhone may have been "the most successful product of all time."⁹ The iPhone's success has given rise to a vibrant app ecosystem. Its App Store hosts over two million apps and 20 million registered developers and generates \$50 billion in

THEORIES OF HARM PAPER SERIES: PAPER 2, 22 (2020), <https://som.yale.edu/sites/default/files/DTH-Apple-new.pdf>.

5. Apple Inc. v. Pepper, 139 S. Ct. 1514 (2019).

6. See Nick Statt, *Epic Games Is Suing Apple*, THE VERGE (Aug. 13, 2020, 3:46 PM EDT), <https://www.theverge.com/2020/8/13/21367963/epic-fortnite-legal-complaint-apple-ios-app-store-removal-injunctive-relief>; Stephen Nellis, *Developers Sue Apple over App Store Practices*, REUTERS (June 4, 2019), <https://www.reuters.com/article/us-apple-antitrust/developers-sue-apple-over-app-store-practices-idUSKCN1T5249>. Released after a substantially completed manuscript of this Note and the completed version of its sister paper, both of which were widely circulated publicly starting in May 2020, Epic Games' complaint against Apple parallels many of this Note's arguments. See generally Complaint, Epic Games v. Apple, 2020 U.S. Dist. LEXIS 154231 (N.D. Cal. Aug. 24, 2020) (No. 20-05640); Kotapati et al., *supra* note 4 (making SSRN Top Ten downloaded papers in multiple antitrust categories in May 2020 through August 2020).

7. See *infra* Section IV.A.

8. Jack Nicas, *Apple Is Worth \$1,000,000,000,000. Two Decades Ago, It Was Almost Bankrupt.*, N.Y. TIMES (Aug. 2, 2018), <https://www.nytimes.com/2018/08/02/technology/apple-stock-1-trillion-market-cap.html>.

9. Ben Thompson, *Amazon's New Customer*, STRATECHERY (June 19, 2017), <https://stratechery.com/2017/amazons-new-customer>.

sales a year.¹⁰ These apps have “ignited a cultural, social and economic phenomenon that changed how people work, play, meet, travel and so much more” according to Apple.¹¹

Apple’s increasing abuse of its dominance, however, threatens to enfeeble this vibrant market as it leverages its control over a mobile economy bottleneck to extract rent and tilt the app market in its favor. In the ostensible U.S. mobile platform duopoly between Apple’s iOS and Google’s Android, significant differentiation has already reduced head-to-head competition: Apple emphasizes privacy, security, and user experience while Google offers lower price points at the expense of monetizing user attention.¹² The strength of Apple’s ecosystem further gives the iPhone maker de facto monopoly power: Apple holds 71% of the mobile app platform market by revenue; iPhone users’ switching costs are over 50 times higher than a 5% app price increase; and Apple has been able to raise iPhone prices by 33% without losing sales.¹³

Thanks to Apple’s control of iOS and the App Store, the only place iPhone users can legally download apps, the company is able to mandate all third-party in-app purchases of digital goods to go through its payment system and charge a 30% tax on all these transactions.¹⁴ This “Apple tax” extracts extra profits from users already paying for an expensive phone, even as it leads to higher app prices and reduced innovation in an increasingly important mobile economy.¹⁵

Moreover, Apple has disadvantaged rivals and favored its own apps by blocking certain rivals entirely, downgrading competitors’ discovery and

10. Jack Nicas & Keith Collins, *How Apple’s Apps Topped Rivals in the App Store It Controls*, N.Y. TIMES (Sept. 9, 2019), <https://www.nytimes.com/interactive/2019/09/09/technology/apple-app-store-competition.html>; Ingrid Lunden, *App Store Hits 20M Registered Developers and \$100B in Revenues, 500M Visitors per Week*, TECHCRUNCH (June 4, 2018), <https://techcrunch.com/2018/06/04/app-store-hits-20m-registered-developers-at-100b-in-revenues-500m-visitors-per-week>.

11. *The App Store Turns 10*, APPLE (July 5, 2018), <https://www.apple.com/newsroom/2018/07/app-store-turns-10>.

12. *See Market Study into Mobile App Stores*, NETH. AUTH. FOR CONSUMERS & MKS 27–28 (Apr. 11, 2019), <https://www.acm.nl/sites/default/files/documents/market-study-into-mobile-app-stores.pdf> [hereinafter *Dutch ACM Study*].

13. *See infra* Part IV.

14. *See infra* Part V. As of the last substantive update of this Note but after the writing of its substantially completed manuscript, Apple announced that it would reduce its tax rate to 15% for developers earning less than \$1 million per year starting January 1, 2021. *See* Jack Nicas, *Apple Halves Its App Store Fee for the Smaller Companies*, N.Y. TIMES (Nov. 18, 2020), <https://www.nytimes.com/2020/11/18/technology/apple-app-store-fee.html>. Although a welcome change, this move will affect only 5% of Apple’s App Store revenue and thus does not make a significant difference to Apple’s policy overall. *See id.*

15. *Id.*

promotions, and limiting others' access to key iPhone features, in some cases right after copying their apps.¹⁶ As Apple aggressively pushes into services, rival apps face growing risks of distorted competition. Since around 2016, Apple's business model has gradually shifted from primarily making and selling smartphone hardware towards relying more on the services iPhone users consume.¹⁷ It has launched video streaming, news, and video-game subscriptions and piloted its own mobile payment and music apps.¹⁸ Apple's services revenue has more than quadrupled in absolute terms over the past decade to over \$50 billion annually, now representing 22.8% of Apple's total sales from 8.3% in 2011.¹⁹ It is also a much more profitable segment with a 65.4% gross margin, more than doubling the hardware products' 30.3% margin.²⁰ As Apple increasingly relies on its services revenue and more frequently attempts to tilt the mobile platform playing field to protect this cash cow, the threat from its exclusionary, self-preferencing conduct looms larger than ever. In conjunction with the discriminatory²¹ application of its 30% tax, Apple's conduct not only harms competition on the iOS platform but also weakens major multihoming apps such as Spotify who are critical to competition between mobile platforms. Apple's conduct further deters the rise

16. See *infra* Section VI.A.

17. See Ben Thompson, *The iPhone and Apple's Services Strategy*, STRATECHERY (Sept. 11, 2019), <https://stratechery.com/2019/the-iphone-and-apples-services-strategy>.

18. Chaim Gartenberg, *How Apple Makes Billions of Dollars Selling Services*, THE VERGE (Mar. 20, 2019, 9:00 AM EDT), <https://www.theverge.com/2019/3/20/18273179/apple-icloud-itunes-app-store-music-services-businesses>; Mark Gurman, *Apple Reinvention as Services Company Starts for Real Monday*, BLOOMBERG (Mar. 23, 2019), <https://www.bloombergquint.com/technology/apple-s-reinvention-as-a-services-company-starts-for-real-monday>.

19. See Kif Leswing, *Apple Issues New Rules for App Store that Will Impact Streaming Game Services from Google and Microsoft*, CNBC (Sept. 11, 2020, 1:00 PM EDT), <https://www.cnbc.com/2020/09/11/apple-app-store-new-rules-will-affect-google-stadia-microsoft-xcloud.html>; Press Release, Apple, *Apple Reports Second Quarter Results* (Apr. 30, 2020), <https://www.apple.com/newsroom/2020/04/apple-reports-second-quarter-results> (showing \$13.3B services revenue and \$58.3B total revenue in 2020 Q2); Neil Cybart, *The Apple Services Machine*, ABOVE AVALON (May 15, 2018), <https://www.aboveavalon.com/notes/2018/5/15/the-apple-services-machine> (estimating \$9B services revenue for 2011 Q4 trailing twelve months); *Apple Reports Fourth Quarter Results*, APPLE (Oct. 18, 2011), <https://www.apple.com/newsroom/2011/10/18Apple-Reports-Fourth-Quarter-Results> (showing \$108B revenue for 2011).

20. See APPLE, CONDENSED CONSOLIDATED STATEMENTS OF OPERATIONS (UNAUDITED) (2020), https://www.apple.com/newsroom/pdfs/FY20_Q2_Consolidated_Financial_Statements.pdf (disclosing sales and costs of products and services respectively for three months ended on March 28).

21. Apple's apps are not subject to the 30% cost disadvantage. See *infra* Section VI.A.III.

of future platforms, an effect reminiscent of Microsoft's exclusion of Netscape to preserve its Windows monopoly.²²

Apple's practices violate antitrust law as they damage competition and consumer welfare, the promotion of which are key objectives of the Sherman Act.²³ Apple's story is also a case study of how a platform can stand as a gatekeeper between hundreds of millions of consumers and small businesses, while garnering immense power by purposefully building a walled garden that platform participants cannot escape due to their resource limitations.²⁴ This story provides important lessons for governing all tech platforms. In particular, the vast scope and magnitude of potential and actual abuse of platform dominance in a world of ubiquitous multilayered dynamic networks, as Apple's example reveals,²⁵ ought to ring the alarm bell for anyone concerned with consumer welfare.

However, current judicial doctrines governing antitrust law present significant obstacles to enforcement against tech platforms' abuse of dominance. Influenced by traditional antitrust thinking dominated by what is known as the Chicago School, courts today espouse an overly benign view of dominant firm behavior that takes too lightly the risk of leveraging dominance in adjacent markets and denying competitors reasonable access to essential services.²⁶ These judicial doctrines limit the viability of antitrust lawsuits against tech giants, even when they are abusing their dominance to extract monopoly rents at the expense of competition and innovation.

This Note makes the antitrust case against Apple, investigates how the rise of consumer platforms like Apple poses critical challenges to the U.S. regime of competition law and policy, and calls for a rethinking of the antitrust toolbox. It proceeds in seven parts. Part II exposes the doctrinal inadequacies of current U.S. monopoly law. Part III explores the main features of the modern consumer platform economy. Part IV frames the impact of these features in antitrust terms to show Apple's market power and dominance. Part V analyzes Apple's illegal tying arrangement regarding its in-app purchase system. Part VI shows how Apple prolongs and expands its monopoly over the smartphone platform market. Part VII refutes claimed efficiency justifications for Apple's conduct. Part VIII concludes with suggestions for reforming antitrust doctrines and reprioritizing enforcement strategies for the twenty-first century.

22. *See infra* Section VI.C.

23. *See infra* Parts V–VI.

24. *See infra* Sections III.A–C.

25. *See infra* Sections III.D, VI.A.

26. *See infra* Part II.

Tech platforms have played a key role in driving innovations for the modern consumer economy, but they are now increasingly becoming obstacles. To build a future of fair competition and protect consumer welfare, antitrust law is in urgent need of transformative rethinking.

II. THE MYTHICAL BENIGN MONOPOLIST

Traditional antitrust thinking in the United States has been built on the back of an enterprise-facing manufacturing economy. Leading theorists of the Chicago School, the most influential school of thought in U.S. antitrust law, developed their expertise by analyzing big manufacturers.²⁷ As a result, a set of economic assumptions rooted in the industrial economy have become entrenched in the current antitrust thinking that do not fit the modern consumer platform economy.

In particular, traditional antitrust theories often assume rationality, market efficiency, and lack of barriers to entry²⁸ because proponents of these theories tend to focus on sophisticated firms of similar power in a world with rare network effects. For example, Robert Bork's hugely influential book *The Antitrust Paradox*, the poster child of the Chicago School,²⁹ routinely mentions rational and efficient economic models involving a "widget manufacturer" in a market of "100 firms of equal size" selling to "1,000 well-informed purchasers."³⁰ Bork also sneers at the idea of entry barriers, calling them "ghosts" that "do not exist."³¹ These assumptions have resulted in an overly benign view of dominant firms as ones that only exist because of efficiencies from scale, ones that are always at risk of being toppled by would-be competitors³²—a view inconsistent with today's increasing concentration of tech giants who maintain dominance despite their serious problems.³³

27. See, e.g., Aaron Director & Edward H. Levi, *Law and the Future: Trade Regulation*, 51 NW. U.L. REV. 281 (1956–57); Sam Peltzman, *Aaron Director's Influence on Antitrust Policy*, 48 J.L. & ECON. 313 (2005).

28. See Daniel L. Rubinfeld, *On the Foundations of Antitrust Law and Economics*, in HOW THE CHICAGO SCHOOL OVERSHOT THE MARK 51, 54 (Robert Pitofsky ed., 2008) (discussing the Chicago School's faith in efficient market and likelihood of entry).

29. See generally George L. Priest, *The Abiding Influence of the Antitrust Paradox*, 31 HARV. J.L. & PUB. POL'Y 455 (2008).

30. See ROBERT BORK, *THE ANTITRUST PARADOX* 96–97 (1978).

31. *Id.* at 310.

32. See Patrice Bougette, Marc Deschamps & Frederic Marty, *When Economics Met Antitrust: The Second Chicago School and the Economization of Antitrust Law*, 16 ENTER. & SOC'Y 313, 333 (2015).

33. See GEORGE J. STIGLER CTR. FOR THE STUDY OF THE ECON. & THE STATE, COMMITTEE FOR THE STUDY OF DIGITAL PLATFORMS MARKET STRUCTURE AND ANTITRUST

Under this sanguine view, business efficiencies rather than monopoly profits motivate monopolists to expand into adjacent markets.³⁴ Often known as the “one monopoly profit” theory, it argues that unless the monopolist’s leveraging is efficient, it cannot extract additional profit from a second market as buyers pay for the two products as a package.³⁵ Buyers will consume less of the package if the second product gets more expensive because of the leveraging. The monopolist will thus not be able to increase its profit and hurt competition under the theory unless it can save costs and sell the second product more cheaply than competitors, in which case it is not an antitrust problem.

Heavily influenced by the Chicago School, current antitrust doctrines construe monopoly leveraging and refusal to deal—two important categories of monopolistic exclusionary conduct—too narrowly, often leaving damaging anticompetitive practices untouched. Courts today thus frequently attack monopolization claims with these assumptions of yesteryear.

Under *Verizon Communications v. Law Offices of Curtis V. Trinko, LLP*, the most recent Supreme Court case on leveraging, the use of monopoly power in one market to acquire competitive advantage in another must either meet the standard of actually monopolizing or having “a dangerous probability of success” in monopolizing the second market in order to violate Section 2 of the Sherman Act.³⁶ This formulation creates a high burden for showing monopoly leveraging in two ways. First, it leaves out monopoly leveraging *without probable monopolization* of the second market even when it is nonetheless significantly harmful (including monopoly leveraging into new dynamic network markets) as Sections V.B and VI.A-C will show. Second, it wrongfully excludes the defensive leveraging discussed in Section VI.C that prolongs monopoly in the *primary* market.

The Court’s demand for at least a dangerous probability of monopolization creates a practical requirement to define the relevant secondary market(s) affected by leveraging.³⁷ Market definition is required to show alleged

SUBCOMMITTEE REPORT 11 (2019), <https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure-report.pdf>.

34. See Richard A. Posner, *The Chicago School of Antitrust Analysis*, 127 U. PA. L. REV. 925, 927 (1979) (“[V]ertical integration must be motivated by a desire for efficiency rather than for monopoly.”).

35. See HERBERT HOVENKAMP, *FEDERAL ANTITRUST POLICY: THE LAW OF COMPETITION AND ITS PRACTICE* 426, 565 (5th ed. 2016).

36. *Verizon Commc’ns v. Law Offs. of Curtis V. Trinko, LLP*, 540 U.S. 398, 415 n.4 (2004) (citing *Spectrum Sports, Inc. v. McQuillan*, 506 U.S. 447, 459 (1993)).

37. See *Spectrum Sports*, 506 U.S. at 455–56; *United States v. Microsoft Corp.*, 253 F.3d 34, 81 (D.C. Cir. 2001).

monopolization under current antitrust doctrine.³⁸ Such inquiries can be fact-intensive and costly even for cases involving merely one market,³⁹ let alone the several if not dozens of markets often affected by monopoly platforms' leveraging as Apple's example in Section VI.A will show. Requiring market definition in this context can thus significantly dampen antitrust plaintiffs' incentives and weaken their ability to bring suits against dominant platforms, despite the substantial anticompetitive harm caused by dominant platforms' conduct. Economists and dissenting Justices on the Supreme Court have already pointed out that market definition in general is but an imprecise tool for helping to find anticompetitive harm and is thus unnecessary when there is proof of actual detrimental effects.⁴⁰ To maintain such a superfluous but costly threshold for plaintiffs, in particular for leveraging claims involving multiple markets, would likely further give tech platforms significant leeway to abuse their dominance.

The Supreme Court's undue skepticism springs from its concern that allowing monopoly leveraging as an independent claim of exclusionary conduct "might chill competition, rather than foster it."⁴¹ Lower courts have shared this sentiment. The Seventh Circuit, for example, has stated that "[t]he problem with 'monopoly leveraging' as an antitrust theory is that the practice cannot increase a monopolist's profits."⁴² Both statements bear clear hallmarks of the Chicago School's charitable view of monopolists, which this Note will show is misplaced. Courts' outdated views threaten to leave anticompetitive conduct untouched, impacting hundreds of billions of economic activities on platforms such as Apple, Amazon, Google, and Facebook, to the detriment of consumers.

Like the leveraging doctrine, courts today strongly disfavor refusal to deal claims. Illegal refusal to deal occurs when a monopolist refuses to engage with customers, suppliers, or competitors or only offers very unreasonable terms, with the effect of excluding rivals from the market and thereby harming consumers.⁴³ Although a common intuition is that firms should be free to

38. See *United States v. Grinnell Corp.*, 384 U.S. 563, 570–71 (1966).

39. See Patrick R. Ward, *Testing for Multisided Platform Effects in Antitrust Market Definition*, 84 U. CHI. L. REV. 2059, 2070–73 (2017).

40. See *Ohio v. Am. Express*, 138 S. Ct. 2274, 2296 (2018) (Breyer, J., dissenting); Steven C. Salop, *The First Principles Approach to Antitrust, Kodak, and Antitrust at the Millennium*, 68 ANTITRUST L.J. 187 (2000); Jonathan B. Baker, *Market Definition: An Analytical Overview*, 74 ANTITRUST L.J. 129, 131 (2007); Louis Kaplow & Carl Shapiro, *Antitrust*, in 2 HANDBOOK OF LAW AND ECONOMICS 1073, 1091 (A. Mitchell Polinsky & Steven Shavell eds., 2007).

41. *Spectrum Sports*, 506 U.S. at 458.

42. *Schor v. Abbott Lab'ys.*, 457 F.3d 608, 611 (2006).

43. See HOVENKAMP, *supra* note 35, at 387–96.

choose with whom they want to deal, the Supreme Court itself has held that this “does not mean that the right is unqualified.”⁴⁴ *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*,⁴⁵ the beginning of modern refusal to deal cases, offers an example of how such conduct can be problematic. In that case, Skiing Co., a monopolist ski resort, suddenly ended a joint marketing program with a rival despite the arrangement’s long-standing history, which suggested the arrangement’s likely profitability.⁴⁶ Finding no valid business reason behind the abrupt change which sacrificed Skiing Co.’s profits, the Supreme Court concluded that it was used to exclude the competitor and therefore violated antitrust law for illegal monopolization.⁴⁷

Increasingly, however, courts recognize refusal to deal claims only in very limited circumstances after the Supreme Court’s decision in *Trinko*.⁴⁸ In that case, the Court also pondered over a refusal to deal claim and announced a general right for a firm “freely to exercise [its] own independent discretion as to parties with whom [it] will deal,” casting doubt on the “uncertain virtue of forced sharing” and focusing on “the difficulty of identifying and remedying anticompetitive conduct by a single firm.”⁴⁹ The *Trinko* Court severely curtailed *Aspen Skiing*: it placed the case “at or near the outer boundary of § 2 liability” and emphasized the importance of showing the end of a prior course of dealing contrary to a firm’s short-term profitability in *Aspen*.⁵⁰ As the Eleventh Circuit has observed, “*Trinko* now effectively makes the unilateral termination of a voluntary course of dealing a requirement for a valid refusal-to-deal claim.”⁵¹ Such a narrow interpretation of the doctrine focuses on but one instance of harmful refusal to deal, missing the broader underlying principle of *Aspen* against anticompetitive exclusionary conduct. As the rest of the Note will show, this narrow view again ignores the risks of tech platforms’ denial of service. These risks stem from both tech platforms’ importance as today’s digital infrastructure, upon which economic activities worth hundreds of billions of dollars rely, and the kind of installed-base opportunism in which entrenched platforms can engage.

The remaining Parts of the Note highlight the problem with courts’ narrow interpretation of monopolization by studying how the new market dynamics

44. *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 601 (1985).

45. *Id.*

46. *See id.* at 587–95.

47. *See id.* at 608–11.

48. *See Verizon Commc’ns v. Law Offs. of Curtis V. Trinko, LLP*, 540 U.S. 398, 408–10 (2004).

49. *Id.* at 408.

50. *Id.* at 410.

51. *Covad Commc’ns Co. v. BellSouth Corp.*, 374 F.3d 1044, 1049 (11th Cir. 2004).

of the consumer platform economy upend traditional antitrust assumptions. Then the Note demonstrates how Apple has abused its dominance and caused harm to consumers and competition to the extent of billions of dollars, which could go unrecognized under current antitrust law. Without substantial doctrinal reform, current antitrust law can give free rein to manipulation by giant tech platforms. Competition in the entire digital economy is at stake.

III. THE CONSUMER PLATFORM ECONOMY

The American economy in the twenty-first century is vastly different than half a century ago, when Bork and his Chicago School peers started to dominate antitrust law thinking with economic theories developed for the industrial economy. Based on its share of the gross domestic product (GDP), the manufacturing sector has more than halved between 1967 and 2017.⁵² The share of consumer-facing sectors, on the other hand, has expanded by over 40% in the same period.⁵³

Moreover, consumer-facing companies have reached unprecedented scale. The largest firms today are more likely to be consumer-oriented than not: among America's Fortune 20 firms, consumer-facing businesses jumped from 25% of the list in 1967 to 60% in 2019.⁵⁴ Big tech companies such as Apple,

52. *Compare Interactive Access to Industry Economic Accounts Data: GDP by Industry (Historical)*, BUREAU OF ECON ANALYSIS, https://apps.bea.gov/iTable/iTable.cfm?reqid=147&step=51&isuri=1&startyear=1967&table_list=5&endyear=1967&valuationtype=b&theta=1&codelist=22r (last visited Jan. 4, 2021) (hereinafter *Economic Data 1967*) (showing the 1967 manufacturing share of GDP as 25.3%), *with Industry Economic Account Data: GDP by Industry*, BUREAU OF ECON. ANALYSIS, https://apps.bea.gov/iTable/iTable.cfm?reqid=150&step=3&isuri=1&table_list=5&series=a&first_year=2017&columns=ii&scale=-99&last_year=2017&categories=gdp&xind=&thetable=&rows=22r,gdp,pvt,11,111ca,113ff,21,211,212,213,22,23,31g,33dg,321,327,331,332,333,334,335,3361mv,3364ot,337,339,31nd,311ft,313tt,315al,322,323,324,325,326,42,44rt,441,445,452,4a0,48tw,481,482,483,484,485,486,487os,493,51,511,512,513,514,fire,52,521ci,523,524,525,53,531,hs,ore,532rl,prof,54,5411,5415,5412op,55,56,561,562,6,61,62,621,622,623,624,7,71,711as,713,72,721,722,81,g,gf,gfg,gfgd,gfng,gfe,gs,gslg,gsle,pgood,pserv,ict (last visited Jan. 4, 2021) (hereinafter *Economic Data 2017*) (showing the 2017 manufacturing share of GDP as 11.2%).

53. *Compare Economic Data 1967*, *supra* note 52, *with Economic Data 2017*, *supra* note 52 (showing a decline from 48.5% to 68.3%, with sectors other than traditional and government productions considered consumer-facing sectors).

54. *Compare A Database of 50 Years of FORTUNE's List of America's Largest Corporations*, FORTUNE, https://archive.fortune.com/magazines/fortune/fortune500_archive/full/1967 (last visited Jan. 4, 2021) (including five consumer-facing auto, electronics, and telecommunications firms and fifteen energy, manufacturing, and enterprise software firms), *with Fortune 500*, FORTUNE, <https://fortune.com/fortune500/2019/search> (last visited Jan. 4, 2021) (including twelve consumer-facing retail, electronics, telecommunications, auto, healthcare, and software firms and eight energy, financial, and wholesale healthcare firms).

Microsoft, Amazon, Facebook, and Google—all with huge consumer-facing businesses—are worth trillions or hundreds of billions of dollars.⁵⁵

Technologies such as the internet and smartphones have drastically reduced transaction costs on the supply side and have created huge network effects. They have made platforms that aggregate hundreds of millions, if not billions, of consumers much more plausible than it was in the era of industrial manufacturing. On the demand side, however, this lopsided power balance introduces often prohibitive transaction costs for platform participants who are much smaller and less sophisticated than the giant platforms, preventing the former from making economic decisions solely based on the merits.

As this Part demonstrates, the rise of the consumer platform economy has brought about seismic economic changes impacting antitrust law. These changes have made dominant tech companies much more powerful and their anticompetitive conduct much more harmful than traditionally assumed.

A. CONSUMERS AS KEY ECONOMIC ACTORS

Traditional antitrust law and economics have usually assumed rational actors because of their focus on firms, which tend to have the capability of being rational due to economies of scale, repeat transactions, and competitive selection.⁵⁶ Consumers, on the other hand, may lack the transactional sophistication and informational capability to be largely rational, leaving them vulnerable to monopolistic exploitation.

First, consumers are less able than enterprises to discover market information before making purchases, especially for products with add-on attributes. Enterprises often have dedicated personnel to carry out sophisticated analysis of their purchase decisions.⁵⁷ In contrast, individual consumers do not generally have such capabilities—especially when, for example, millions of heterogeneous apps exist in the Apple App Store. This gives platforms greater power to raise add-on prices.

Second, consumers have fewer incentives to bear the information cost. Enterprise equipment is generally much more expensive than consumer

55. See Jack Nicas, *Apple Reaches \$2 Trillion, Punctuating Big Tech's Grip*, N.Y. TIMES (Aug. 19, 2020), <https://www.nytimes.com/2020/08/19/technology/apple-2-trillion.html>; Melissa Pistilli, *10 Top Technology Stocks by Market Cap*, INVESTING NEWS (Nov. 19, 2020), <https://investingnews.com/daily/tech-investing/top-technology-stocks> (showing that Apple, Microsoft, Amazon, Alphabet, and Facebook were worth \$2.08 trillion, \$1.63 trillion, \$1.58 trillion, \$1.2 trillion, and \$782 billion, respectively).

56. See Mark Armstrong & Steffen Huck, *Behavioral Economics and Antitrust*, in 1 THE OXFORD HANDBOOK OF INTERNATIONAL ANTITRUST ECONOMICS 205–06 (2015).

57. See Carl Shapiro, *Aftermarkets and Consumer Welfare: Making Sense of Kodak*, 63 ANTITRUST L.J. 483, 493 (1995).

products, and firms tend to buy in large quantities. Relatively small enterprise investments in discovering information are thus more worthwhile, as they lead to large savings in procurement cost. Consumers, however, primarily engage in one-off purchases of consumer-price goods; extensive research is often not worth the effort for them, even as the aggregate harm from inefficient pricing for billions of consumers is comparable or greater than that for firms.

Even potential competitive price-cutting and educational advertising cannot eliminate inefficient, “shrouded” add-on prices when close substitutes exist, according to leading behavioral economics literature.⁵⁸ Low-price competitors who try to inform consumers of high add-on prices (e.g., airline bag fees) from rivals will lead them to cheaper substitutes and incur the cost of education, thereby becoming less profitable.⁵⁹ For smartphone platforms, this can occur when they offer subscription apps that are more expensive than their web counterparts due to platform fees. Even if one platform can offer cheaper options than another, it would not do so since this would only drive consumers out of smartphone platforms and to the web, hurting all industry players. Inefficient high app prices can thus persist.

Given the high costs of discovering information about platform markets, consumers will find it hard to compare *ex ante* the total costs of using the platform itself and the services provided on the platform. For example, iPhone users may not be aware of how expensive apps are on iOS when making smartphone purchase decisions. This lack of awareness impedes competition between smartphone platforms that could have resulted in lower app prices.

B. SMALL BUSINESSES AND APP DEVELOPERS

The rise of consumer platforms has also brought about many small businesses that serve individual consumers. Apple has twenty million developers creating apps for users; Amazon has about three million active marketplace sellers offering goods to buyers; and YouTube has fifty million content creators delivering videos to viewers.⁶⁰ Most of these developers,

58. See generally Xavier Gabaix & David Laibson, *Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets*, 121 Q.J. ECON. 505 (2006).

59. See *id.*

60. See Ingrid Lunden, *App Store Hits 20M Registered Developers and \$100B in Revenues, 500M Visitors Per Week*, TECHCRUNCH (June 4, 2018), <https://techcrunch.com/2018/06/04/app-store-hits-20m-registered-developers-at-100b-in-revenues-500m-visitors-per-week>; *Distribution of Active Amazon Marketplace Sellers Worldwide in 2019, by Country*, STATISTA, <https://www.statista.com/statistics/1086651/amazon-3p-seller-global-distribution> (last visited Jan. 4, 2021); *YouTube by the Numbers: Stats, Demographics & Fun Facts*, OMNICORE, <https://www.omnicoreagency.com/youtube-statistics> (last updated Oct. 28, 2020).

sellers, and content creators are very small businesses (one to five people).⁶¹ These small businesses suffer from many of the same resource limitations that consumers have, giving platforms even more power for monopolistic exploitation. This Section focuses on smartphone app developers, but these lessons can apply to small businesses on other platforms as well.

First, developers invest in platform-specific skills that are hard to transfer. Mobile app developers have to learn coding skills and conventions which can vary significantly across platforms.⁶² Becoming a proficient developer for a new platform can take six to fifteen months.⁶³ This means very few developers can afford to switch platforms, much less develop for multiple ones at the same time—only 8.8% of iOS developers also work on Android or Windows, for example.⁶⁴ This friction creates significant switching costs for small businesses such as app developers—probably also YouTube creators and to a lesser extent Amazon retailers—which makes platforms much more powerful than dominant firms in traditional industries.

Second, small businesses lack the transactional sophistication to negotiate contracts. Traditional antitrust scholars have argued that buyers have strong incentives to obtain contractual protections against future seller exploitation—for example via warranty protections, rental or lease of the product, and long-term service contracts.⁶⁵ However, the average developer studio consisting of only one to five people would not have the bargaining power to negotiate with tech platforms for individually tailored terms. As a result, platforms have acquired extraordinary power to exploit small businesses and harm competition.

61. See, e.g., MACSTADIUM, TRENDS IN IOS DEVOPS: A SURVEY OF IOS DEVELOPERS FROM THE 2018 APPLE WORLDWIDE DEVELOPERS CONFERENCE (WWDC) & ALTCONF (2018), https://uploads-ssl.webflow.com/5c0953da973d4d733aab924e/5c0953da973d4d689aab9427_MacStadium-iOS-DevOps-Survey.pdf (showing that 66% of iOS developer teams have 1-10 members and that the average size is 3.8 for those having 2-10 members); *Key Metrics of Amazon.com Marketplace Sellers in the United States in 2019*, STATISTA, <https://www.statista.com/statistics/1086637/amazoncom-3p-seller-metrics-usa> (last visited Jan. 4, 2021) (noting that over 80% of Amazon active sellers have annual sales below \$100,000).

62. See, e.g., JonnyB, *What Does It Take to Become an Android Developer?*, MEDIUM (May 22, 2018), <https://medium.com/devslopes-blog/what-does-it-take-to-become-an-android-developer-fbd31d06a4f4>.

63. See Martin Campbell-Kelly, Daniel Garcia Swartz, Richard Lam & Yilei Yang, *Economic and Business Perspectives on Smartphones as Multi-Sided Platforms*, 39 TELECOMMS. POL'Y 717, 728 (2015).

64. See Sami Hyrynsalmi, Arho Suominen & Matti Mäntymäki, *The Influence of Developer Multi-Homing on Competition Between Software Ecosystems*, 111 J. SYS. & SOFTWARE 119, 123 (2016) (“[T]he number of [seller-level] multi-homers varies from 8.8% for the Apple App Store . . .”).

65. See Shapiro, *supra* note 57, at 488–91.

C. ECOSYSTEM LOCK-INS

The third feature of the consumer platform economy is the ubiquity of product ecosystems that integrate both vertically and horizontally, including software as well as costly hardware. These ecosystems can generate high switching costs and strong barriers to competition that give platforms strong market power and prevent effective competition.

Firms such as Apple have been strategically designing their product portfolios and building up walls between ecosystems to increase switching costs. In Apple's case, Steve Jobs himself strategized that the company should "[t]ie all of our products together, so we further lock customers into our ecosystem" in an internal email on "2011: Holy War with Google."⁶⁶ Further, Apple offers multiple hardware products (iPhone, iPad, Mac computer, Apple Watch, HomePod smart speaker, etc.) with data and features that work across devices to improve utility of owning multiple devices.⁶⁷ Platforms also offer downstream services unique to particular platforms, such as Apple's Apple Music, Apple Pay, and Apple's Podcasts. As a result, the average Apple user in the United States spends around \$802 per year, equivalent to the cost of owning two to three iPhones, on Apple products and services.⁶⁸ Google and Amazon employ similar tactics with offerings such as Amazon Prime Video, Echo smart speaker, Gmail, and Google Home. When users own multiple pieces of the same ecosystem, the cost of switching becomes higher. Economists found the cost of switching one's smartphone operating system (OS) is around \$250 in South Korea, for example, from "application

66. Don Reisinger, *Steve Jobs Wanted to Further Lock Customers' into Apple's Ecosystem*, CNET (Apr. 2, 2014), <https://www.cnet.com/news/steve-jobs-wanted-to-further-lock-customers-into-apples-ecosystem>.

67. See *Use Continuity to Connect Your Mac, iPhone, iPad, iPod Touch, and Apple Watch*, APPLE, <https://support.apple.com/en-us/HT204681> (last visited Jan. 4, 2021).

68. The \$802 per user spending is derived from Apple's U.S. sales in 2019 from iPhone users divided by user number (105 million), assuming the United States accounts for 80% of Apple's \$117 billion Americas revenue and 90% of Apple users own at least one iPhone. Thus, per user spending = $117M \times 80\% / (105M / 90\%) = \802 . Comparison with iPhone cost is based on iPhone average price of \$800 and a two-to three-year upgrade cycle. See APPLE INC., CONDENSED CONSOLIDATED STATEMENTS OF OPERATIONS (UNAUDITED) (2019), https://s2.q4cdn.com/470004039/files/doc_financials/2019/q4/Q4-FY19-Consolidated-Financial-Statements.pdf; *Apple Grows iPhone Share in US, Despite Overseas Challenge*, EMARKETER (Mar. 12, 2019), <https://www.emarketer.com/content/apple-grows-iphone-share-in-us-despite-overseas-challenge>; Press Release, Consumer Intel. Rsch. Partners, LLC, iPhone 11 Takes Over Where iPhone XR Left Off (Apr. 22, 2020), at 2, <https://files.constantcontact.com/150f9af2201/3ece3965-9d56-4c2e-8ed8-c7e49b73de66.pdf>; Evan Niu, *The Great Irony of Apple's iPhone Price Increases*, MOTLEY FOOL (Dec. 6, 2018), <https://www.fool.com/investing/2018/12/06/the-great-irony-of-apples-iphone-price-increases.aspx>.

purchasing cost, accessory purchasing cost, and uncertainty from the possibility of additional post-transition payment increase”—even excluding incompatibility of other platform-specific smart devices people own.⁶⁹ Given Apple's strong product ecosystem in the United States, the cost is likely higher here for iOS. Facing such high switching costs, Apple's iOS retention rate in the United States is around 90%, meaning nine in ten iPhone users do not switch to alternative smartphones.⁷⁰

D. MULTILAYERED DYNAMIC NETWORKS

Another feature of the consumer platform economy is the multilayered, dynamic network structure of tech platforms. Network effects allow a firm's market power to grow exponentially, as it scales in ways often unrelated to the quality of the underlying product offering.⁷¹ Tech platforms are special in this respect due to the ubiquity of such networks being layered on top of one another in fast-growing markets. This market structure not only gives platforms extraordinary market power but also creates perverse incentives for platforms to expand monopoly power from one network market to another, causing self-propelling and irreversible harm to competition.

Apple's smartphone platform, for example, is a two-sided market with strong network effects; more users attract more developers to a growing market, while more developers creating more apps attracts more users.⁷² This effect creates enormous collective action problems when any individual developer or user wants to exit for not liking Apple's offerings. They cannot realistically coordinate with a critical mass of fellow developers or users (who number in the hundreds of millions) to quit together unless Apple's offerings become exceptionally terrible. Furthermore, they cannot create an alternative platform to attract other developers and users even if they can improve on the product offering because the presence of other developers and users are a

69. Yuri Park & Yoonmo Koo, *An Empirical Analysis of Switching Costs in the Smartphone Market in South Korea*, 40 TELECOMMS. POL'Y 307, 313–14 (2016). The dollar value is based on the exchange rate of 1 South Korean won to 0.00081 USD on April 24, 2020.

70. Ben Thompson, *Apple's China Problem*, STRATECHERY (Jan. 7, 2019), <https://stratechery.com/2017/apples-china-problem/>.

71. See, e.g., Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479 (1998); David S. Evans, *The Antitrust Economics of Multi-Sided Platform Markets*, 20 YALE J. ON REG. 325 (2003).

72. See Daniel D. Garcia-Swartz & Florencia Garcia-Vicente, *Network Effects on the iPhone Platform: An Empirical Examination*, 39 TELECOMMS. POL'Y 877, 889 (2015) (finding that each extra app is associated with 271–386 additional users and that each 1000 additional users are associated with 2.5–3.6 additional apps).

critical piece of the platform's utility. This magnifies already significant user switching costs⁷³ and creates often insurmountable barriers to entry.

Moreover, other platforms can exist on top of the App Store. Apple Pay, for example, grows more popular and dominant as more merchants accept it, which spurs user adoption that again feeds back into greater merchant uptake. Spotify works similarly for music listeners and artists, where more users attract both more future users to listen to the playlists they create and more artists to make music for them, and these artists and their songs in turn attract more users. The data that platforms gather from a growing user base offers further economies of scale—as the use of platforms like Spotify and Netflix increases, they gain more insight into user preferences and are thus better able to improve their product offerings.⁷⁴

Downstream network effects can distort the competitive incentive of the platform operator upon entry into those markets. When network strength matters more than product superiority,⁷⁵ the platform operator may plausibly twist the rules of the downstream market it controls such that they favor the platform operator and help it dominate, even with inferior products, by depriving rivals of key inputs needed to acquire sufficient scale to succeed.⁷⁶ A classic example of how network effects can result in such a suboptimal market structure is the QWERTY keyboard, which was designed with an outdated technology but remains the popular format because manufacturers and users are locked into this technology, despite being 36% less efficient than modern alternatives.⁷⁷ Inefficient monopoly leveraging can thus yield higher quality-adjusted prices and fewer choices, leading to consumer welfare losses.⁷⁸

Multilayered network markets exist extensively in today's consumer platform economy. Apple's exclusionary, self-preferencing tactics in their mobile payment service, music streaming, gaming platform, and other network markets discussed in Parts V-VI demonstrate that tech platforms today can

73. See text accompanying note 69.

74. See, e.g., Jon Markman, *Netflix Harnesses Big Data to Profit from Your Tastes*, FORBES (Feb. 25, 2019), <https://www.forbes.com/sites/jonmarkman/2019/02/25/netflix-harnesses-big-data-to-profit-from-your-tastes/#55ee2c2f66fd>.

75. See Lemley & McGowan, *supra* note 71.

76. See Michael D. Whinston, *Tying, Foreclosure, and Exclusion*, 80 AM. ECON. REV. 837, 838–39 (1990); Dennis W. Carlton & Michael Waldman, *The Strategic Use of Tying to Preserve and Create Market Power in Evolving Industries*, 33 RAND J. ECON. 194, 196–97 (2002); W. Brian Arthur, *Competing Technologies, Increasing Returns, and Lock-In by Historical Events*, 99 ECON. J. 116 (1989).

77. See Jan Noyes, *The QWERTY Keyboard: A Review*, 18.3 INT'L J. MAN-MACHINE STUD. 265, 278 (1983); Shumin Zhai, Michael Hunter & Barton Allen Smith, *Performance Optimization of Virtual Keyboards*, 17 HUM.-COMPUT. INTERACTION 229 (2002).

78. See Whinston, *supra* note 76, at 839.

and do take advantage of the anticompetitive opportunities offered by multilayered network markets.

IV. APPLE'S DOMINANCE: DE FACTO MONOPOLY

With often prohibitive information and switching costs on top of strong network effects, Apple holds a powerful dominance over the mobile platform market. This Part translates the features of the consumer platform economy into antitrust terms by examining Apple's dominance and showing that Apple has market power to impose anticompetitive terms on other market players.

Market power is required for both illegal tying and monopolization,⁷⁹ two legal claims that capture the core anticompetitive nature of Apple's conduct. The Supreme Court has required market definition to show market power⁸⁰ with the relevant market being the "arena within which significant substitution in consumption or production occurs."⁸¹ Here we are concerned with the U.S. market for mobile app platforms, which host services including digital goods within smartphone apps.⁸²

Power in the relevant market means "some special ability . . . to force a purchaser to do something that he would not do in a competitive market."⁸³ Courts have found indirect evidence of market power to include a high market share, barriers to entry, and locked-in customers.⁸⁴ Direct evidence of actually

79. *See* Ill. Tool Works v. Indep. Ink, 547 U.S. 28, 46 (2006); United States v. Grinnell Corp., 384 U.S. 563, 570–71 (1966).

80. *See* Ohio v. Am. Express, 138 S. Ct. 2274, 2285 (2018).

81. PHILLIP E. AREEDA & HERBERT HOVENKAMP, 2B ANTITRUST LAW ¶ 530a (4th ed. 2019).

82. Overall mobile app services include spending on IAP goods/services, paid apps, in-app advertising, and in-app physical goods and services (such as toilet paper bought on Amazon or Uber rides). *See Choosing a Business Model*, APPLE DEVELOPER, <https://developer.apple.com/app-store/business-models> (last visited Jan. 4, 2021). Both paid apps and IAP goods are included in our market definition because they are generally monetized through mobile app stores' built-in monetization tools, whereas the other two categories are excluded because they tend to go through outside third-party systems and have different business models, both of which are not easily substitutable.

83. *Jefferson Par. Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 13–14 (1984).

84. *See id.* at 17; *Grinnell*, 384 U.S. at 571 (inferring monopoly from dominant market share); *United States v. Microsoft Corp.*, 253 F.3d 34, 54–55 (D.C. Cir. 2001) (finding that an "applications barrier to entry" supports Microsoft's monopoly power over the computer operating system market); *Eastman Kodak v. Image Tech. Servs.*, 504 U.S. 451, 473–78 (1992) (finding monopoly power from customer lock-ins/aftermarket power).

exercising control over price or excluding competition provides further support.⁸⁵

While the monopoly power standard is more stringent than market power for tying,⁸⁶ this Part shows that Apple satisfies both tests with its 71% market share, switching costs 50 times higher than a 5% app price increase, and ability to profitably increase iPhone price by 33%.

A. MARKET SHARE

Apple owns 71% of the U.S. mobile app platform market by revenue.⁸⁷ Its 62–86% global market share for the past decade further corroborates its durable dominance.⁸⁸ Courts have found 59% and 69% market shares to be sufficient for tying.⁸⁹ For monopolization, a market share over 70% generally establishes prima facie monopoly power, and a market share between 50–70% can constitute monopoly power when combined with substantial barriers to entry in the market.⁹⁰ Apple's market share alone thus leads to a strong inference for sufficient market power for both tying and monopolization.

85. See *Kodak*, 504 U.S. at 477–78 (“It is clearly reasonable to infer that Kodak has market power to raise prices and drive out competition . . . [from] direct evidence that Kodak did so.”).

86. See *id.* at 480.

87. Reed Albergotti, *How Apple Uses Its App Store to Copy the Best Ideas*, WASH. POST (Sept. 5, 2019), <https://www.washingtonpost.com/technology/2019/09/05/how-apple-uses-its-app-store-copy-best-ideas>. Indeed, Apple has just about half of the installed smartphone user base in the United States. See S. O’Dea, *U.S. Smartphone Subscriber Share by Operating Platform 2012–2020, by Month*, STATISTA (Nov. 25, 2020), <http://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states>. But Apple’s revenue share is likely more important for measuring Apple’s power to control users and developers’ economic decisions. Developers care about the potential revenue from their apps as they are in the business to make money. Users, on the other hand, want to have as many apps and as many quality apps as possible. Their willingness to pay for in-app digital goods (which reveals their preferences) is thus a good sign of their demand for digital goods.

88. J. Clement, *App Spend Distribution Between Apple App Store and Google Play 2012–2018*, STATISTA (June 17, 2020), <https://www.statista.com/statistics/259510/revenue-distribution-between-the-apple-app-store-and-google-play>.

89. See, e.g., *Bodet v. Charter Commc’ns*, Civil Action No. 09-3068 Section “F,” 2010 U.S. Dist. LEXIS 87088, at *18–19 (E.D. La. 2010) (finding a 69% market share sufficient for inferring plausible market power); *In re Cox Enters., Set-Top Cable TV Box Antitrust Litig.*, No. 09-ML-2048-C, 2010 U.S. Dist. LEXIS 58417, at *19–20 (W.D. Okla. 2010) (finding 59% sufficient for inferring plausible market power); cf. *Dickson v. Microsoft Corp.*, 309 F.3d 193, 209 n.20 (4th Cir. 2002) (finding 30% insufficient for inferring plausible market power).

90. See 3B AREEDA & HOVENKAMP, *supra* note 81, ¶ 801a. The term “monopoly” in the antitrust sense does not necessarily mean a firm with 100% market share. Rather it often refers to what economists call a dominant firm. See *id.* ¶ 801. The distinction is perhaps partly a result of antitrust law’s purpose to prevent dominant firms from becoming perfect economic

B. BARRIERS TO ENTRY

As discussed in Part III, user and developer lock-ins, strong network effects, and economies of scale and scope in the form of broad ecosystems—factors courts have recognized in antitrust cases—create significant barriers to entry that protect Apple.⁹¹ Strong lock-in features, in particular, further strengthen Apple's power over both consumers and developers by increasing switching costs. The Supreme Court held in *Eastman Kodak* “[i]f the cost of switching is high, [buyers] who already have purchased the equipment, and are thus ‘locked in,’ will tolerate some level of [supracompetitive prices],” which is a sign of seller's market power.⁹²

As Section III.C has mentioned, iPhone users face switching costs of at least \$250⁹³ and rarely switch to a different platform—the iPhone's retention rate is consistently in the high 80% in the United States, and more recently it has been above 90%.⁹⁴ The \$250 estimate only factors in “application purchasing cost, accessory purchasing cost, and uncertainty from the possibility of additional post-transition payment increase.”⁹⁵ Apple's strong product ecosystem likely poses even higher costs due to the incompatibility of the other Apple-specific smart devices that people own. Even if iPhone apps see a 5% price increase—a threshold antitrust enforcement agencies often use to infer monopolist status if the move does not reduce profits⁹⁶—which would

monopolies. The law's focus regarding market power is thus often on a firm's ability to exclude competitors and become a perfect monopoly.

91. See *United States v. Microsoft Corp.*, 253 F.3d 34, 55 (D.C. Cir. 2001) (finding an “applications barrier to entry” from “chicken-and-egg” effects of consumer preference for operating systems with many applications and developer preference to write software for a substantial customer base—essentially network effects—which “protects a dominant operating system irrespective of quality”); *Image Tech. Servs. v. Eastman Kodak Co.*, 125 F.3d 1195, 1208 (9th Cir. 1997) (finding entry barriers in part due to economies of scale); *Kodak*, 504 U.S. at 476 (finding lock-ins to contribute significantly to market power).

92. 504 U.S. at 476–77.

93. See text accompanying note 69.

94. See Joe Rossignol, *CIRP Says iOS Loyalty ‘Hit the Highest Levels We’ve Ever Measured’ Last Quarter*, MACRUMORS (Jan. 28, 2019), <https://www.macrumors.com/2019/01/28/cirp-iphone-android-loyalty-4q18/>; Gordon Gottsegen, *Almost All iPhone Users Will Buy Another iPhone*, *Says Survey*, CNET (May 18, 2017), <https://www.cnet.com/news/apple-iphone-92-percent-retention-morgan-stanley-survey>. Similar reasons give Android strong lock-ins as well. Both platforms thus likely have power beyond their market share numbers, making them arguably two quite distinct markets.

95. Park & Koo, *supra* note 69, at 313–14.

96. See *Horizontal Merger Guidelines*, DEP'T OF JUST. §§ 4.1.1–2 (Aug. 19, 2010), <https://www.justice.gov/atr/horizontal-merger-guidelines-08192010>.

amount to \$5 per user given the average app spending of \$100,⁹⁷ users would likely tolerate the price hike as their switching costs would be over 50 times higher. Even with a 30% price increase, switching costs would still be more than eight times higher, allowing Apple to maintain supracompetitive profits to a significant extent.

These barriers thus prevent competition from easily accessing Apple's users, making the company's power over its user base and in turn the developers who covet these users much stronger than the 71% market share implies.

C. DIRECT EVIDENCE

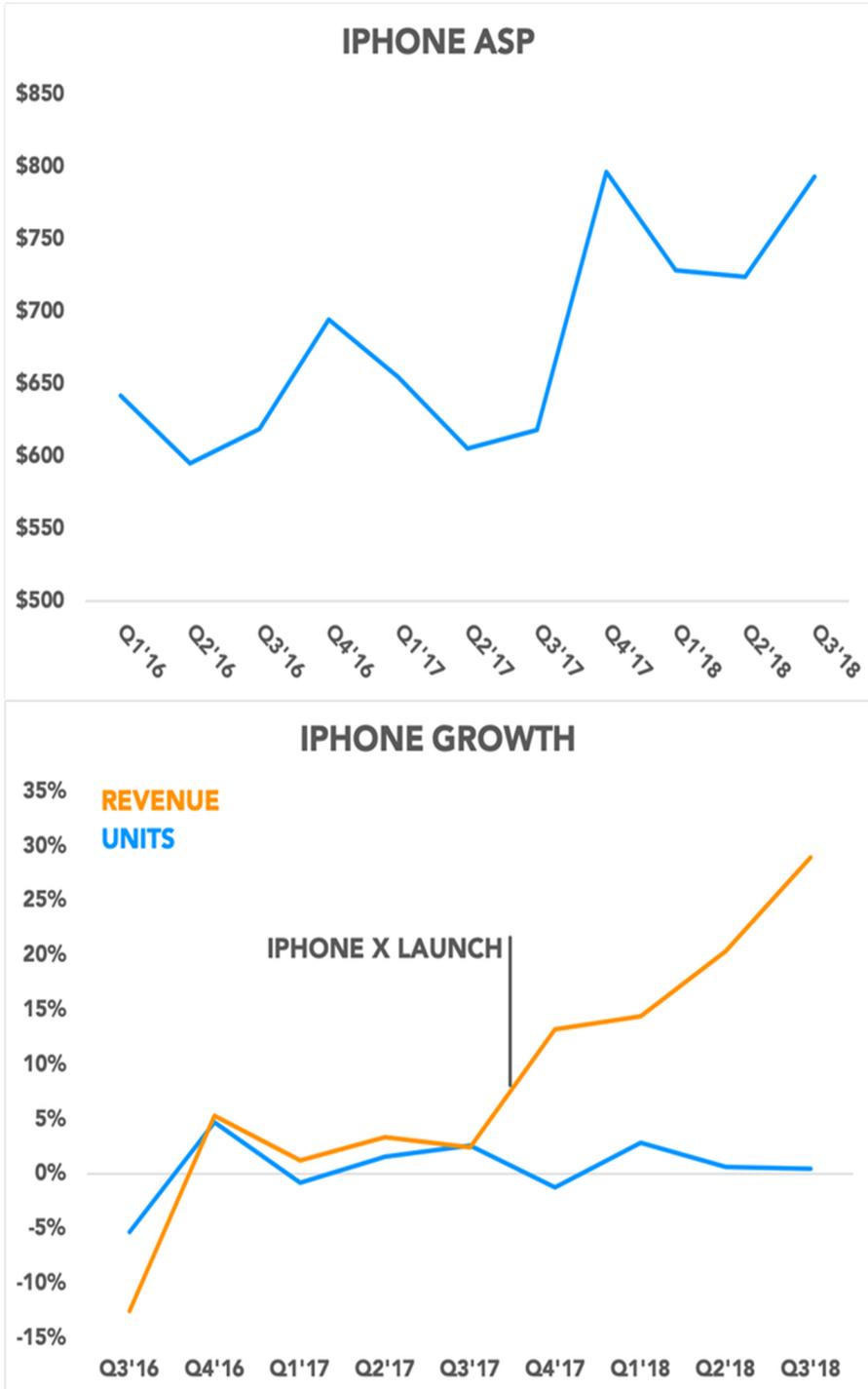
Direct evidence of the actual exercise of control over prices or the actual exclusion of competition from the relevant market can more strongly indicate monopoly power.⁹⁸ Despite raising iPhone's prices by around 33% over the past few years, Apple continues to see its sales volume remain steady and revenue grow, as Figure 1 shows.⁹⁹

97. See Randy Nelson, *U.S. iPhone Users Spent an Average of \$100 on Apps in 2019, Up 27% from 2018*, SENSOR TOWER (Mar. 25, 2020), <https://sensortower.com/blog/revenue-per-iphone-2019>.

98. See *Eastman Kodak v. Image Tech. Servs.*, 504 U.S. 451, 477–78 (1992) (“It is clearly reasonable to infer that Kodak has market power to raise prices and drive out competition . . . [from] direct evidence that Kodak did so.”); *FTC v. Ind. Fed’n of Dentists*, 476 U.S. 447, 460–61 (1986) (using direct proof to show market power).

99. See Niu, *supra* note 68.

Figure 1: iPhone Average Selling Price and Sales



This pricing power is against the backdrop of the iPhone's narrowing advantage over Android phones. For example, CNET has given Samsung's Galaxy S20 (its latest flagship phone as of this writing) a score of 8.7 compared to a similarly priced iPhone model's 8.8.¹⁰⁰ Yet after Samsung raised its premium phones' prices, its smartphone profits dropped by 42% due to "weak sales momentum . . . and stagnant demand for [its] premium products."¹⁰¹ The contrast demonstrates Apple's unique market power stemming from its platform lock-ins that in many ways make iOS a distinct market over which Apple has monopoly control.¹⁰²

Further, Apple has indeed exercised its power to exclude rivals, as Section VI.A discusses, and sustained supracompetitive prices. The continued existence of an inefficient 30% in-app purchase fee, as Part V details, is direct evidence of Apple's power. The Seventh Circuit has held "[market power] means power over price The best way to show power over price is to establish directly that the price of the tied package is higher than the price of components sold in competitive markets."¹⁰³ Google's Android allows certain developers to distribute their paid in-app digital goods (e.g., ebooks and downloaded songs) without using its in-app purchase services,¹⁰⁴ effectively eliminating any associated fees. Tinder, for example, recently decided to not use Google's payment system as to avoid any fee, whereas it still has to use Apple's in-app purchase system and pay the Apple tax on iOS.¹⁰⁵ Epic Games, the maker of Fortnite (one of the most popular video games in history), has similarly exited Google's Play Store and now uses its own payment system to avoid fees; but it had to tolerate Apple's in-app purchase system for two years

100. See Scott Stein, *Apple iPhone XS Max Review*, CNET (Dec. 17, 2018), <https://www.cnet.com/reviews/apple-iphone-xs-max-review>; Jessica Dolcourt, *Galaxy S20 5G Review: Top-Shelf Specs, But Plenty of Room for Refinement*, CNET (Mar. 13, 2020), <http://www.cnet.com/reviews/samsung-galaxy-s20-5g-review>.

101. See Catherine Shu, *Samsung Posts 55.6% Drop in Second-Quarter Profit as It Copes with Weak Demand and a Trade Dispute*, TECHCRUNCH (July 31, 2019), <https://techcrunch.com/2019/07/30/samsung-posts-55-6-drop-in-second-quarter-profit-as-it-cope-with-weak-demand-and-a-trade-dispute>.

102. See *Kodak*, 504 U.S. at 473–78 (finding distinct market from strong lock-ins and high switching costs).

103. *Will v. Comprehensive Accounting Corp.*, 776 F.2d 665, 671–72 (7th Cir. 1985) (citations omitted).

104. See GOOGLE PLAY, *Monetization and Ads*, PLAY CONSOLE HELP, <https://play.google.com/about/monetization-ads> (last visited Jan. 4, 2021) (listing a variety of monetization strategies, including paid distribution, in-app products, subscriptions, and ad-based models).

105. See Olivia Carville, *Tinder Bypasses Google Play Joining Revolt Against App Store Fee*, BLOOMBERG (July 19, 2019), <https://www.bloomberg.com/news/articles/2019-07-19/tinder-bypasses-google-play-joining-revolt-against-app-store-fee>.

because it is forbidden to use alternative payment mechanisms on iPhone.¹⁰⁶ This disparity clearly indicates that Apple has some unique power that others in the market simply do not have.¹⁰⁷

The story of Nintendo in the video game console market provides a telling parallel. With a similar market structure where Nintendo serves both as the gaming platform operator and games distributor for third-party developers, Nintendo charged developers essentially \$44 per game sold around late 80s when it had dominance in the gaming console market and tied game cartridge manufacturing to distribution.¹⁰⁸ Nintendo eventually had to cut its royalty rate to \$7 per game due to both FTC scrutiny that undid the tie and successive competition from Sega, Sony, and Microsoft.¹⁰⁹ In contrast with Apple's basically constant rate of around 30%, this precipitous decline shows that only with market power can a platform maintain a supracompetitive, inefficient price for a tied service.

Combined with indirect evidence of Apple's market power such as dominant market share and barriers to entry, direct evidence such as its unique

106. See Nick Statt, *Fortnite for Android Will Ditch Google Play Store for Epic's Website*, THE VERGE (Aug. 3, 2018), <https://www.theverge.com/2018/8/3/17645982/epic-games-fortnite-android-version-bypass-google-play-store>. Epic's Fortnite was also removed from the iOS App Store in August 2020 after Epic sued Apple. Fortnite's daily active users on iOS have declined by over 60% since then, supporting Apple's economic power over Epic. See Sean Hollister, *Read Epic's New, Full Argument Why a Court Should Force Apple to Reinstate Fortnite*, THE VERGE (Sept. 5, 2020), <https://www.theverge.com/2020/9/5/21423889/fortnite-epic-apple-preliminary-injunction-filing-ios-mac>.

107. Although Apple has offered a reduced 15% fee for subscription apps starting their second year after maintaining a uniform 30% tax for eight years, this is only a very partial exception, and it may more properly be interpreted as an attempt to price discriminate, appease sophisticated developers, and deter them from opposing and changing the rule. In fact, Apple's overall take rate has only changed from 30% to 26.4% as a result of the 15% exception according to an estimate. See *Dedicated to the Best Store Experience for Everyone*, APPLE, <https://www.apple.com/ios/app-store/principles-practices> (last visited Jan. 4, 2021); Roger Fingas, *Apple Announces It Will Offer App Store Subscriptions to All Apps, Take Smaller 15% Cut*, APPLEINSIDER (June 08, 2016), <https://appleinsider.com/articles/16/06/08/apple-announces-it-will-offer-app-store-subscriptions-take-smaller-15-cut>; *Apple Discloses Key App Store Financial Data Point, Hulu Revises Pricing, Aetna and Apple Announce Watch Partnership*, ABOVE AVALON (Jan. 29, 2019), <https://www.aboveavalon.com/dailypremiumupdate/2019/1/29/apple-discloses-key-app-store-financial-data-point-hulu-revises-pricing-aetna-and-apple-announce-watch-partnership>.

108. See Andrei Hagiu, *Microsoft Xbox: Changing the Game?* 6-13 (Harv. Bus. Sch., Case No. 9-707-501, 2007) (on file with author).

109. See *id.*; Andrew Quemere, *The People Versus Mario: The FTC's Forgotten Investigation into Nintendo in the '90s*, MUCKROCK (Feb. 2, 2017), <https://www.muckrock.com/news/archives/2017/feb/02/people-versus-mario-ftcs-investigation-nintendo>; DAVID S. EVANS, ANDREI HAGIU & RICHARD SCHMALENSE, *INVISIBLE ENGINES: HOW SOFTWARE PLATFORMS DRIVE INNOVATION AND TRANSFORM INDUSTRIES* 126 (2008).

pricing power, actual exclusion, and sustained supracompetitive prices tend to strongly support Apple's dominance. When consumers and developers find it hard to switch away even in the face of price hikes and quality degradation, Apple's dominance over this sticky user base thus makes the platform a de facto monopoly.

V. TYING: FORCING THE APPLE TAX

Apple has abused its dominance by tying the distribution of digital goods to its proprietary in-app purchase (IAP) payment system to impose a 30% tax and extract supracompetitive profits, leading to higher app prices and reduced innovation through illegal tying. At the core of the tying doctrine is a forced, inefficient, and often unwanted combination of transactions achieved through imposition of market power.¹¹⁰ This Part will show the IAP tie is illegal and hurts consumers and developers alike to the extent of billions of dollars.

Apple's App Store is the sole channel through which iPhone users can download iOS apps.¹¹¹ Third-party (i.e., non-Apple) app developers have to submit the apps they have created to Apple for its review and approval.¹¹² Third-party apps cannot reach iPhone consumers without following Apple's rules and guidelines, including those governing app monetization.¹¹³

Beyond the basic functionality provided by downloading an app, developers may sell bonus features or digital goods within the app,¹¹⁴ such as "subscriptions, in-game currencies, game levels, access to premium content, or unlocking a full version."¹¹⁵ This is an important way for developers to monetize their creations, generating tens of billions of dollars a year in revenue.¹¹⁶ However, for in-app digital goods to be distributed to purchasing users, developers must configure their apps so that all purchases of the digital

110. See *Jefferson Par. Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 12 (1984).

111. See *App Store Review Guidelines* § 3.2.2, APPLE DEVELOPER, <https://developer.apple.com/app-store/review/guidelines> (last visited Jan. 4, 2021) [hereinafter *App Store Review Guidelines*] (forbidding apps "similar to the App Store"). The App Store is the sole channel unless users employ technical hacks known as "jailbreaking," which has always been a small niche and has increasingly fallen out of use these days. See Lorenzo Franceschi-Bicchierai & Brian Merchant, *The Life, Death, and Legacy of iPhone Jailbreaking*, VICE (June 29, 2017), <https://www.vice.com/en/article/8xa4ka/iphone-jailbreak-life-death-legacy>.

112. See *App Store Review Guidelines*, *supra* note 111.

113. See *id.* § 3.

114. See *In-App Purchase*, APPLE DEVELOPER, <https://developer.apple.com/in-app-purchase> (last visited Jan. 4, 2021).

115. *App Store Review Guidelines*, *supra* note 111, § 3.1.

116. See J. Clement, *Worldwide Gross App Revenue of The Apple App Store from 2017 to 2019*, STATISTA (Jan. 2020), <https://www.statista.com/statistics/296226/annual-apple-app-store-revenue>.

goods go through Apple's IAP system, which processes the transactions.¹¹⁷ With very limited exceptions, Apple takes a 30% cut from all such third-party IAP transactions for using its payment system.¹¹⁸ For example, for every ten dollars consumers pay for a Pandora streaming music subscription, three dollars go to Apple. This 30% fee operates essentially like a tax, allowing Apple to profit from developer revenues often only tenuously related to Apple's efforts.

The App Store's rules forbid developers from offering alternative payment mechanisms or even providing information about them: "Apps may not use their own mechanisms to unlock content or functionality, such as license keys, augmented reality markers, QR codes, etc. Apps and their metadata may not include buttons, external links, or other calls to action that direct customers to purchasing mechanisms other than in-app purchase."¹¹⁹ Apps violating these rules will be rejected or removed from the App Store. The rules thus forcefully combine the IAP system with the distribution of paid digital goods and serve to enable and protect Apple's tax revenue.

A. ESTABLISHING THE IAP TIE

Section 1 of the Sherman Act prohibits tying in restraint of trade.¹²⁰ In addition to market power discussed in Part IV, courts generally require four factors in finding illegal tying: (1) two separate products or services are involved; (2) the sale of one product or service is conditioned on the purchase of another; (3) anticompetitive effect in the market for the tied product affects not an insubstantial amount of interstate commerce; and (4) procompetitive efficiencies of the tie do not outweigh its anticompetitive effect.¹²¹ The sections below analyze how the IAP tie meets the first three elements of the judicial test for illegal tying and restrains competition (while Section V.A analyzes how the IAP tie meets the fourth element).

117. *See id.*

118. *See App Store Review Guidelines, supra* note 111, § 3; SPOTIFY, *Five Fast Facts, TIME TO PLAY FAIR*, <https://timetoplayfair.com/facts> (last visited Jan. 4, 2021). Apple announced that it would reduce its tax rate to 15% for developers earning less than \$1 million per year starting January 1, 2021, but this move will affect only 5% of Apple's App Store revenue and thus does not make a significant difference to Apple's policy overall. *See Nicas, supra* note 14.

119. *App Store Review Guidelines, supra* note 111, § 3.1.1.

120. Other prohibitions on tying arrangements include Clayton Act § 3, 15 U.S.C. § 1, 14, and the Federal Trade Commission Act § 5, 15 U.S.C.A. § 45; *see also* HOVENKAMP, *supra* note 35, at 534, 537 (discussing the statutory scheme prohibiting tying in restraint of trade).

121. *See* 10 AREEDA & HOVENKAMP, *supra* note 81, ¶¶ 1702, 1760 (4th ed. 2019); *see also* United States v. Microsoft Corp., 253 F.3d 34, 84–97 (D.C. Cir. 2001) (en banc) (holding that rule of reason and in particular consideration of efficiencies may be needed in the case of tying software products).

1. *Separability*

For two services to be separate, “there must be sufficient [buyer] demand so that it is efficient for a firm to provide [one service] separately from [another].”¹²² Courts have found sufficient separate demand when the two offerings have previously been sold separately and when other industry suppliers sell them separately.¹²³

Apple had itself offered distribution of in-app subscriptions independent of IAP services until 2011.¹²⁴ In fact, many subscription app developers protested the bundling when the rule was introduced.¹²⁵ Moreover, Android allows certain apps to distribute digital goods (e.g., ebooks and downloaded songs) without using its IAP services.¹²⁶ Separate demand thus does exist for IAP and distribution.

2. *Forceful Conditioning*

Courts require proof of coercion to establish forceful conditioning,¹²⁷ for which often “a formal agreement is . . . sufficient.”¹²⁸ Apple requires the use of IAP by fiat through the App Store rules, forbidding all alternative payment mechanisms.¹²⁹ As developers cannot distribute apps without following these rules, coercion is clearly established.

122. *Eastman Kodak v. Image Tech. Servs.*, 504 U.S. 451, 462 (1992).

123. *See id.*; *Associated Press v. Taft-Ingalls Corp.*, 340 F.2d 753, 759–64 (6th Cir. 1965).

124. *See Why You Should Fight Apple’s Subscription Extortion*, TREEHOUSE (Feb. 15, 2011), <https://blog.teamtreehouse.com/why-you-should-fight-apples-subscription-extortion>; Press Release, Apple, Apple Launches Subscriptions on the App Store (Feb. 15, 2011), <https://web.archive.org/web/20110307215013/https://www.apple.com/pr/library/2011/02/15appstore.html> (announcing the policy); John Gruber, *Dirty Percent*, DARING FIREBALL (Mar. 1, 2011), https://daringfireball.net/2011/03/dirty_percent.

125. *See, e.g.*, TREEHOUSE, *supra* note 124 (“I’d . . . NOT [pay] 30% of all my revenue going forward [for some IAP services].”).

126. *See* GOOGLE PLAY, *Monetization and Ads*, DEVELOPER POL’Y CTR., <https://play.google.com/about/monetization-ads> (last visited Jan. 4, 2021); *see also* Olivia Carville, *Tinder Bypasses Google Play Joining Revolt Against App Store Fee*, BLOOMBERG (July 19, 2019), <https://www.bloomberg.com/news/articles/2019-07-19/tinder-bypasses-google-play-joining-revolt-against-app-store-fee> (“[To avoid Android’s IAP services] Match . . . changed the payment method in-app . . . Others have instead forced subscribers back to their own websites to enter payment information.”).

127. *See Paladin Assocs. v. Mont. Power Co.*, 328 F.3d 1145, 1159 (9th Cir. 2003).

128. *Ungar v. Dunkin’ Donuts of Am., Inc.*, 531 F.2d 1211, 1224 (3d Cir. 1976).

129. *See* text accompanying note 119.

B. CONSUMER HARM: TAXING THE APP ECONOMY

Recent cases increasingly require an inquiry into anticompetitive effects in the tied product market, even for per se tying claims.¹³⁰ Specifically, courts consider an alleged anticompetitive arrangement's impact on price, quality, quantity, and innovations.¹³¹

Here, the consumer-side harm is two-fold. First, despite already paying high prices for the iPhone, users must pay higher prices for apps as developers pass on the overcharge; their experience then suffers from reduced quality and innovations in the iPhone experience. For example, the following table shows that nearly all major music streaming apps are 30% more expensive on iOS than Android; the exception is Apple Music as Apple does not pay the 30% fee itself.¹³²

Table 1: iOS Subscription Prices for Major Music Streaming Apps

| | Spotify* | Pandora | Tidal | YouTube Music | Apple Music |
|--|----------|---------|---------|---------------|-------------|
| iOS | \$12.99 | \$12.99 | \$12.99 | \$12.99 | \$9.99 |
| Android | \$9.99 | \$9.99 | \$9.99 | \$9.99 | N/A |
| *Before Spotify stopped in-app iOS subscriptions in 2016 | | | | | |

When developers don't charge 30% higher, perhaps because their customers are more price sensitive, developers are left with less to invest in improving quality. This loss can amount to tens of billions of dollars that Apple

130. *See, e.g.,* *Princo Corp. v. Int'l Trade Comm'n*, 616 F.3d 1318, 1338 (Fed. Cir. 2010); *E & L Consulting v. Doman Indus.*, 472 F.3d 23, 32 (2d Cir. 2006); HOVENKAMP, *supra* note 35, at 535. Illegal tying also requires that a "not insubstantial amount of commerce" in the tied product must be affected, which is a de minimus test easy to meet for the IAP processing market worth billions of dollars. *See, e.g.,* *Tic-X-Press v. Omni Promotions Co.*, 815 F.2d 1407, 1419 (11th Cir. 1987) (finding \$10,091 not insubstantial).

131. *See, e.g.,* *Ohio v. Am. Express Co.*, 138 S. Ct. 2274, 2282, 2288–90 (2018) (considering innovation, price, output, and quality effects).

132. The table is as of April 30, 2019—except Spotify, which used to charge 30% more on iOS too but decided to pull out of the IAP system altogether in 2016 and stopped offering subscription on iOS. *See A Timeline: How We Got Here*, SPOTIFY, <https://www.timetoplayfair.com/timeline> (last visited Jan. 4, 2021) [hereinafter *Spotify Timeline*].

has taken from developers.¹³³ Furthermore, the burden of the IAP fee has forced some app publishers to exit the IAP system altogether—Netflix, Spotify, Kindle, and YouTube TV are prominent examples.¹³⁴ Due to Apple's restrictions, these apps cannot even communicate to customers about alternative channels (e.g., developers' websites).¹³⁵ As a result, iPhone users can become frustrated by their inability to acquire digital content available on other platforms.

Second, the IAP-enforced 30% tax has lessened competition in key downstream app markets. For example, Apple exempts Apple Music from the 30% fee while maintaining the tax for its rivals including Spotify. Given these apps' thin margin—Spotify's gross profit margin for its subscription-based services was at 27% in 2018,¹³⁶ for instance—the 30% tax makes it economically unfeasible for Spotify et al. to maintain the \$9.99 price tag on iOS as they do on Android: if Spotify did so, it would be losing money on

133. See Press Release, Apple, Apple Rings in New Era of Services Following Landmark Year (Jan. 8, 2020), <https://www.apple.com/newsroom/2020/01/apple-rings-in-new-era-of-services-following-landmark-year>. Developers have made \$155 billion between 2008 and 2019 through the App Store. Based on a 30% charge by Apple (which means developers retain 70% of all revenue), Apple's App Store revenue would be $155/0.7*0.3 = \$66.4$ billion during this period.

134. See Juli Clover, *YouTube TV Ending Support for App Store Subscriptions in March*, MACRUMORS (Feb. 13, 2020), <https://www.macrumors.com/2020/02/13/youtube-tv-app-store-subscriptions-ending>; Stuart Dredge, *Netflix Joins Spotify in Bypassing Apple in-App Subscriptions*, MUSIC ALLY (Aug. 22, 2018), <https://www.musically.com/2018/08/22/netflix-joins-spotify-in-bypassing-apple-in-app-subscriptions>.

135. See *Spotify Timeline*, *supra* note 132.

136. See Spotify Tech. S.A., Annual Report (Form 20-F) at 50 (Feb. 12, 2019), https://s22.q4cdn.com/540910603/files/doc_financials/annual/SPOT_20F_Master-Master_Exhibits_HTML.pdf. Spotify's gross profit margin for subscription services is likely to be almost the same for its iOS, Android, and PC versions, as its component parts tend not to vary by platform. Spotify's gross profit margin is based solely on (i) the revenue of its streaming services, which include subscription-based premium services and ad-supported free services and (ii) the cost of providing these services, including royalty and distribution costs related to content streaming, but not including, for example, R&D, marketing, and administrative expenses. See *id.* at 48–50, F-10. The margins for premium and ad-supported services are respectively 27% and 18% in 2018, both below 30%. See *id.* at 50. Spotify's royalty costs, the biggest component of its cost of revenue that makes up Spotify's gross profit margin, are calculated based on either a percentage of revenue, a per user amount, or an amount per play. See *id.* at 45. None of these three considerations is likely to change because of the platform (iOS, Android, or PC) on which a song is played/streamed. Spotify does not disclose methodologies for calculating distribution costs for content streaming, the remaining cost component of Spotify's gross profit margin, likely because this component is not significant enough (or else Spotify would be required to disclose its methodologies under securities law's prohibition against material omission). Other than these cost considerations, margin calculations do not discriminate between different sources of revenue.

every subscription it sells. Given Apple Music's already quite dominant position, having surpassed Spotify in paid iOS listeners in the United States,¹³⁷ competitors will understandably tend to shy away in the face of these additional anticompetitive restrictions. Consumers are thus seeing less competition and innovation in the streaming music space. Spotify's recent pivot away from music toward podcasts is a testament to the reduced head-to-head competition for streaming music.¹³⁸

As Apple enters more service markets,¹³⁹ the threat of this 30% tax will grow more prominent, as digital content services often have thin gross margins around or lower than 30%.¹⁴⁰ Subscription apps such as Spotify are critical to consumer experience. About 94% of the top 250 U.S. apps on iOS monetize through in-app subscriptions.¹⁴¹ The star apps are crucial contributors to user consumption—the top 1% of apps generate 93% of all revenue and 80% of new installs.¹⁴² Damaging subscription apps may thus have a significant negative impact on consumer welfare, a key objective of antitrust law.

137. See Anne Steele & Tripp Mickle, *Apple Music Overtakes Spotify in Paid U.S. Subscribers*, WALL ST. J. (Apr. 5, 2019), <https://www.wsj.com/articles/apple-music-overtakes-spotify-in-u-s-subscribers-11554475924>.

138. See Ben Thompson, *Spotify's Podcast Aggregation Play*, STRATECHERY (Feb. 7, 2019), <https://stratechery.com/2019/spotify-s-podcast-aggregation-play> (citing needing “a way to differentiate its service from Apple Music” as a reason for Spotify's podcast strategy). One might argue Spotify's pivot towards podcasts may be procompetitive in the podcast market, given Apple is the biggest player in podcasts as well. However, the streaming music market is much larger—at \$14 billion, it was 20 times larger than the \$700 million podcast market in 2019. See *Music Streaming*, STATISTA, <https://www.statista.com/outlook/209/100/music-streaming/worldwide> (last visited Jan. 4, 2021); A. Guttman, *Podcast Advertising Revenue in the United States from 2015 to 2019*, STATISTA (Sep. 21, 2020), <https://www.statista.com/statistics/760791/us-podcast-advertising-revenue>. A significant anticompetitive impact on streaming music is thus likely to have a much greater effect on consumer welfare than theoretical procompetitive benefits from the nascent podcast market. The net consumer impact is most likely negative to a significant extent as a result.

139. See *supra* text accompanying notes 17–20.

140. For example, between 2010 and 2019, Netflix's gross profit margin was lower than 30% for three years, between 31.3% and 32.3% for another three years, and between 36.3% and 38.3% for the remaining four years. See *Gross Profit Margin for Netflix, Inc.*, FINBOX, https://finbox.com/NASDAQGS:NFLX/explorer/gp_margin (last visited Jan. 4, 2021). Gross margin represents the percentage of total revenue a company has less costs directly related to production and distribution—in Netflix's case, the profit directly related to selling each unit of streaming content without regard to backend corporate costs.

141. Lexi Sydow, *Subscriptions: The Revenue Model Powering Mobile Apps*, APP ANNIE (Feb. 13, 2020), <https://www.appannie.com/en/insights/market-data/subscriptions-powering-mobile-apps>.

142. Katie Williams, *The Top 1% of App Publishers Generate 80% of All New Installs*, SENSOR TOWER (Nov. 21, 2019), <https://sensortower.com/blog/top-one-percent-downloads>.

While Apple may claim its conduct has procompetitive justifications, these claimed efficiencies are either pretextual or not causally necessary for the IAP tie as Section VII.A will show.

Apple has thus abused its power over the iPhone digital goods market in forcing the IAP tie, distorting competition and creating considerable harm to consumers worth tens of billions of dollars without nearly commensurate efficiencies to compensate. It has therefore violated antitrust law for illegal tying.

VI. MONOPOLIZATION: FORTIFYING THE WALLED GARDEN

Apple distributes proprietary apps on the App Store which compete with many third-party developers' apps. Acting both as an umpire and a player, Apple has blocked or impaired rivals and given itself preferential treatment. In doing so, it has illegally maintained, expanded, and prolonged its monopoly in violation of the Sherman Act § 2.

The Sherman Act § 2 prohibits monopolization.¹⁴³ To show monopolization, in addition to establishing monopoly power as discussed in Part III, courts have required a showing of willful acquisition, enhancement, or maintenance of that monopoly power through exclusionary conduct.¹⁴⁴ Courts have not developed a clear general standard of what such exclusionary conduct entails, except that it should be “distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident”¹⁴⁵—that is, anything that is not competition on the merits—and that such conduct “harm[s] the competitive process and thereby harm[s] consumers.”¹⁴⁶ However, certain specific types of conduct have been recognized in case law as exclusionary to varying degrees, including monopoly leveraging and refusal to deal.¹⁴⁷ Yet as discussed in Part II, courts' interpretations of the leveraging and refusal to deal doctrines have become too rigid to accommodate platforms' abuse of dominance, which would fit under

143. See 15 U.S.C. § 2.

144. See *Verizon Commc'ns v. Law Offs. of Curtis V. Trinko, LLP*, 540 U.S. 398, 407 (2004).

145. *United States v. Grinnell Corp.*, 384 U.S. 563, 570–71 (1966).

146. *United States v. Microsoft Corp.*, 253 F.3d 34, 84–97 (D.C. Cir. 2001) (en banc).

147. See *Berkey Photo, Inc. v. Eastman Kodak Co.*, 603 F.2d 263, 275–76 (2d Cir. 1979), *practically overruled*, *Trinko*, 540 U.S. at 415 n.4; *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 603–05 (1985).

the general monopolization standard but may go unrecognized under these two categories of specific exclusionary conduct.¹⁴⁸

This Part will show that Apple's exclusionary, self-preferencing conduct often makes rival apps worse without making its own apps better. By leveraging its dominance into downstream app markets and refusing to provide reasonable access to rivals, Apple not only reduces competition between apps on the iOS platform but also lessens competition between platforms and illegally strengthens Apple's dominance over the mobile platform market, causing irreversible and significant harm to consumers. To address this crisis, courts must reconsider their hostility towards monopoly leveraging and refusal to deal claims.

A. BLOCKING COMPETITORS, RESTRICTING RIVALS, AND SELF-PREFERENCING

This Section outlines Apple's various exclusionary, self-preferencing practices.

1. *Block Competitors*

Apple has rejected every third-party payment app that utilizes iPhone's near-field communication (NFC) chip (which allows convenient offline contactless payment), including the Samsung Pay Mini app.¹⁴⁹ This effectively blocks competitors from entering iOS in a \$100 billion proximity mobile payment market where the company's own Apple Pay service already dominates.¹⁵⁰

Apple has also refused to approve gaming apps that compete with its Apple Arcade game subscription service. It rejected Steam's video game streaming app citing "business conflicts."¹⁵¹ Apple's App Store rules also severely limit rivals' cloud gaming services, making them effectively impractical

148. See text accompanying notes 34–48.

149. See *Dutch ACM Report*, *supra* note 12, at 79, 83.

150. Apple Pay has 47.3% of U.S. proximity mobile payment users whereas Google Pay and Samsung Pay, the next two biggest players, respectively make up 19% and 16.8%. See Amy He, *Apple Pay Dominance Drives Mobile Payment Transaction Volume*, EMARKETER (Oct. 28, 2019), <https://www.emarketer.com/content/apple-pay-dominance-drives-mobile-payment-transaction-volume>.

151. See Nick Statt, *Apple Rejects Valve's Steam Link Game Streaming App over 'Business Conflicts'*, THE VERGE (May 24, 2018), <https://www.theverge.com/2018/5/24/17392470/apple-rejects-valve-steam-link-app-store-ios-game-streaming> (suggesting that Apple rejected Steam's app because the app "allows an iOS user to access another app store, namely Steam, within Apple's tightly controlled ecosystem").

on iOS¹⁵² and hampering innovation in a market otherwise expected to grow into a multi-billion-dollar opportunity by 2024.¹⁵³

Moreover, Apple once removed 11 of the 17 most downloaded apps that helped parents limit the time their children spent on Apple devices, which compete with Apple's own parental control app.¹⁵⁴ Apple claimed these apps could violate user privacy and security.¹⁵⁵ A month later, however, Apple abruptly reversed its policy, specifically permitting technologies previously cited as grounds for removal as long as the apps followed certain guidelines.¹⁵⁶ Small businesses who developed these apps lost millions of dollars following Apple's purge, with some completely shutting down.¹⁵⁷ In addition to having less useful features according to parents, Apple's screen time control tools

152. Before September 2020, only games owned or exclusively licensed by the developer would be allowed, that is, no gaming platform non-exclusively hosting third-party games such as Google's Stadia was allowed. See Mark Gurman, *Apple's App Store Rules Limit Rival Gaming Services While Arcade Runs Free*, BLOOMBERG (Mar. 25, 2020), <https://www.bloomberg.com/news/articles/2020-03-25/google-stadia-nvidia-geforce-microsoft-xcloud-not-on-apple-ios>. Apple tweaked the policies in September 2020 to nominally allow such services, but it still requires every third-party game offered to seek approval through Apple's cumbersome app review process. This new policy effectively makes it impractical to host a cloud-based gaming subscription service on iOS, as these services inherently tend to include a variety of third-party games to be useful at all. See Leswing, *supra* note 19; see also Salvador Rodriguez, *Facebook Launches Cloud Games But Says Apple Won't Allow It on iOS*, CNBC (Oct. 26, 2020), <https://www.cnbc.com/2020/10/26/facebook-launches-cloud-games-on-desktop-and-android-but-not-on-ios.html> (stating that Facebook announced the decision to not launch Facebook cloud gaming on Apple devices citing Apple's "arbitrary" policies).

153. See *Global Cloud Gaming Market is Projected to Grow at 59.0% CAGR During 2019–2024, Reaching a Value of USD 3,107 Million by 2024—ResearchAndMarkets.com*, BUS. WIRE (Jan. 24, 2020), <https://www.businesswire.com/news/home/20200124005414/en/Global-Cloud-Gaming-Market-Projected-Grow-59.0>.

154. See Jack Nicas, *Apple Cracks Down on Apps that Fight iPhone Addiction*, N.Y. TIMES (Apr. 27, 2019), <https://www.nytimes.com/2019/04/27/technology/apple-screen-time-trackers.html>.

155. See Eric Slivka, *Phil Schiller Lays Out Apple's Case for Cracking Down on Screen Time Monitoring Apps*, MACRUMORS (Apr. 27, 2019), <https://www.macrumors.com/2019/04/27/schiller-screen-time-crackdown-mdm> (explaining that Apple removed these apps because some parental management apps used Mobile Device Management technology that "enable[d] a developer to have access to and control over consumers' data and devices").

156. See *Updates to the App Store Review Guidelines*, APPLE DEVELOPER (June 3, 2019), <https://developer.apple.com/news/?id=06032019j>.

157. See Nicas, *supra* note 154; Jack Nicas, *Apple Backs Off Crackdown on Parental-Control Apps*, N.Y. TIMES (June 3, 2019), <https://www.nytimes.com/2019/06/03/technology/apple-parental-control-apps.html> (accounting that two affected small businesses lost \$3 million and more than \$1 million respectively from Apple's move, with one of them having depended on its iPhone app for 80% of the business's revenue).

require the whole family to own iPhones, whereas many affected competing apps allow parents with iPhones to control their children's Android devices.¹⁵⁸

2. *Restrict Rivals*

Apple has restricted promotions of Apple Music competitors. It rejected multiple Spotify app updates for including promotional language such as “get 3 months now for €0.99” or “Get in, Get Premium” while Apple Music sends the same kind of promotions.¹⁵⁹ This deprives consumers of valuable information about lower prices. Similar restrictions are non-existent for Apple. If a user subscribes to Apple's iOS services (such as Apple Music) and then cancels, Apple sends invasive push notifications asking her to re-subscribe.¹⁶⁰ Apple's ads are allowed by default, whereas other developers could not send such promotional notifications at all for almost all of the past twelve years.¹⁶¹ Apple's tactics suppress competition in the multi-billion-dollar iOS streaming music market (where it already holds 70% of paid users) and beyond.¹⁶²

In addition, Apple has for years prohibited third-party music from being used with Siri,¹⁶³ prevented third-party messaging apps from becoming Siri defaults,¹⁶⁴ and allegedly copied third-party apps and suppressed their search results once Apple created its own version.¹⁶⁵

158. *See id.*

159. *Spotify Timeline*, *supra* note 132.

160. *See The Paywalled Garden: iOS Is Adware*, STEVE STREZA (Feb. 17, 2020), <https://stevestreza.com/2020/02/17/ios-adware>.

161. *See id.* Third-party developers have only very recently been allowed to send promotional notifications and only with explicit user permission. *See* Mike Peterson, *Apple Updates App Store Guidelines, Sets iOS 13 SDK Requirement*, APPLE INSIDER (Mar. 4, 2020), <https://appleinsider.com/articles/20/03/04/apple-updates-app-store-guidelines-sets-ios-13-sdk-requirement>.

162. *See* BILLBOARD, *Revenue from Music Streaming in the United States from 2010 to 2019*, STATISTA (Feb. 2020), <https://www.statista.com/statistics/437717/music-streaming-revenue-usa>; Steele & Mickle, *supra* note 137.

163. Apple announced that it would be changing the rule in late 2019 for messaging apps. *See* Mark Gurman, *Apple to Loosen Reins on Outside Messaging, Phone Apps Via Siri*, BLOOMBERG (Oct. 2, 2019), <https://www.bloomberg.com/news/articles/2019-10-02/apple-to-loosen-reins-on-outside-messaging-phone-apps-via-siri>.

164. Apple modified the rule for Spotify after Spotify's antitrust complaint against Apple in March 2019. *See* Tom Warren, *Spotify Is Finally Getting Siri Support with iOS 13*, THE VERGE (Sept. 27, 2019), <https://www.theverge.com/2019/9/27/20886783/spotify-siri-integration-support-ios-13-beta-launch-airpods>; Ek, *supra* note 1.

165. *Cf.* Jon Porter, *Developer Suing Apple for Stealing Idea, Calls on Others to Join the Fight*, THE VERGE (Feb. 5, 2020), <https://www.theverge.com/2020/2/5/21124116/apple-developers-sherlocked-blix-bluelmail-anonymous-email-feature>; Nicas, *supra* note 154.

3. *Self-Preferencing*

Moreover, Apple has a pattern of self-preferencing conduct. Apple's App Store search rankings and editorial recommendations display its proprietary apps much more prominently than similar apps.¹⁶⁶ For example, Apple Arcade, the company's subscription gaming service, gets an entire tab on the App Store, which cannot be turned off.¹⁶⁷

Finally, Apple imposes the 30% tax on third-party apps through the IAP tie but not on Apple's own apps. This eats into the frequently thin profit margins of rival apps and make them less competitive, as discussed in Section V.B.¹⁶⁸

B. RAISE RIVALS' COSTS: EXCLUSIONARY AND COLLUSIVE EFFECTS

In addition to the clear exclusionary effects of Apple blocking competitors in areas such as payment services, its pattern of self-preferencing conduct can raise rivals' costs. Such conduct stifles price competition and weakens competitors for reasons unrelated to their apps' intrinsic quality.

The discriminatory 30% tax and other restrictions mentioned above (which only apply to Apple's competitors but not itself) essentially give Apple a cost advantage of at least 30%.¹⁶⁹ Consequently, even an equally efficient competitor could not compete with Apple on price due to the extra cost burden and would need to be at least 30% more efficient to survive.¹⁷⁰

166. See Jack Nicas & Keith Collins, *How Apple's Apps Topped Rivals in the App Store It Controls*, N.Y. TIMES (Sept. 9, 2019), <https://www.nytimes.com/interactive/2019/09/09/technology/apple-app-store-competition.html> ("Apple's apps have ranked first recently for at least 700 search terms in the store."); see also Mark Gurman, *Apple's Default iPhone Apps Give It Growing Edge Over App Store Rivals*, BLOOMBERG (Oct. 2, 2019), <https://www.bloomberg.com/news/articles/2019-10-02/iphone-ios-users-can-t-change-default-apps-safari-mail-music>; Tripp Mickle, *Apple Dominates App Store Search Results, Thwarting Competitors*, WALL ST. J. (July 23, 2019), <https://www.wsj.com/articles/apple-dominates-app-store-search-results-thwarting-competitors-11563897221>.

167. See Streza, *supra* note 160.

168. See text accompanying note 140.

169. *C.f.* LePage's Inc. v. 3M, 324 F.3d 141, 155 (3d Cir. 2003) ("The anticompetitive feature of package discounting is the strong incentive it gives buyers to take increasing amounts or even all of a product in order to take advantage of a discount aggregated across multiple products. . . . [In this case] even an equally efficient rival may find it impossible to compensate for lost discounts on products that it does not produce.").

170. The discussion below assumes a rival app stays in the IAP system, which is the case for 99.9% of iOS apps. For the rare exceptions such as Spotify, being outside of the IAP system presents a similar cost disadvantage from the additional promotional difficulties or experience degradation as discussed in Section VI.A. The effect on competition thus operates similarly.

The extra cost burden can either exclude rivals who are more efficient by up to 29.9% or produce an implicit collusion where rivals know that price competition would not work and thus raise the price along with Apple. Either way, consumers would suffer from stunted price competition. Such reduced competition also allows Apple to expand its dominance into downstream markets and enhances its monopoly by raising entry barriers. Even if competitors are over 30% more efficient than Apple, they would have less resources to invest in pursuing innovations. This effectively reduces their efficiency advantage by 30% and offsets the additional price cut or quality improvement consumers would otherwise receive.

As Section V.B detailed,¹⁷¹ such conduct has in fact reduced competition from important players such as Spotify and worsened user experience. Even if Apple's proprietary apps are of inferior quality to start with, the unfair advantages they receive would exclude or weaken rivals. These unfair advantages would allow Apple's apps to gain more users, more data, and more complementary players on other sides of the market (e.g., musicians in the case of Apple Music). In such a case, Apple's apps would become more dominant through network effects and scale economies, while users lose out on a potentially higher quality app market as Section III.D discussed.¹⁷²

As Apple enters more service markets,¹⁷³ Apple's exclusionary, self-preferencing conduct would threaten competition more prominently. The harm to competition and consumers means that Apple's conduct fits squarely under the general monopolization standard¹⁷⁴—especially as Apple's proclaimed efficiency justifications prove empty, as demonstrated in Part VII. Perhaps more ominously, Apple's self-preferencing can prolong and extend its monopoly over the smartphone platform market.

C. PROLONG THE PLATFORM MONOPOLY

Through its exclusionary, self-preferencing conduct, Apple further lessens the already feeble competition between iOS and Android and prolongs its own smartphone platform monopoly by weakening cross-platform apps such as Spotify, Facebook, and WeChat.

Cross-platform apps can significantly neutralize the iOS platform's differentiation and undermine Apple's dominance. WeChat provides a case in

171. See text accompanying note 138.

172. Cf. HOVENKAMP, *supra* note 35, at 395–96 (discussing a similar network market involving Windows-compatible server technology where “in a path-dependent world, even a rival's clearly superior or more cost-effective server produced by a rival cannot claim a market unless it achieves compatibility with the rest of the network”).

173. See text accompanying notes 16–20.

174. See text accompanying note 146.

point. Despite early successes, Apple has struggled in China with the rise of WeChat.¹⁷⁵ WeChat is a popular social media app with 1.1 billion monthly active users¹⁷⁶—essentially every smartphone user in China has WeChat. In addition to offering messaging services, it provides all kinds of essential digital services including mobile payment and commerce, news, ride-hailing, and food delivery.¹⁷⁷ WeChat also hosts third-party “mini-programs” that are basically mini-apps which offer services through WeChat’s light interface.¹⁷⁸ WeChat users open mini-programs four times a day on average and spent \$113 billion inside mini-programs in 2019.¹⁷⁹ The growing popularity of mini-apps makes stand-alone apps less important, eroding an important source of iPhone’s differentiation over Android—its stronger lineup of apps. The number of iOS apps downloaded in China in 2019 has fallen 12% from its peak in 2017, compared with a 22% increase in the United States over the same period.¹⁸⁰

WeChat is available on both Android and iOS. Due to WeChat’s essential role in Chinese consumers’ digital lives and the popularity of its mini-programs, the smartphone experience in China is quite similar across smartphone platforms. As a result, Chinese buyers care much less about the underlying operating system when making their smartphone purchase decisions than their Western counterparts—iPhone’s retention rate in China, defined as the percentage of users who do not switch platforms, has dropped to around 50–60% in recent years, almost half of that in the United States at 91%.¹⁸¹

175. Apple’s market share in China has stayed around 10%, compared to 50% or so in the United States. See Samantha Wong, *Smartphone Vendor Market Share in China 2014–2020*, STATISTA (Feb. 2020), <https://www.statista.com/statistics/430749/china-smartphone-shipments-vendor-market-share>; O’Dea, *supra* note 87. Its China revenue has also consistently dropped to around 25.5% lower than a 2015 peak. See Felix Richter, *The Size of Apple’s China Business*, STATISTA (Feb. 18, 2020), <https://www.statista.com/chart/13246/apple-china-revenue>; see also Thompson, *supra* note 70 (showing that Apple had its best numbers in 2015).

176. See Lai Lin Thomala, *Number of Active WeChat Messenger Accounts Q2 2011–Q2 2020*, STATISTA (Nov. 2019), <https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts>.

177. See Connie Chan, *When One App Rules Them All: The Case of WeChat and Mobile in China*, ANDREESSEN HOROWITZ (Aug. 6, 2015), <https://a16z.com/2015/08/06/wechat-china-mobile-first>.

178. See Wayne Ma & Juro Osawa, *How Tencent’s WeChat Poses Creeping Threat to Apple*, THE INFO. (Apr. 14, 2020), <https://www.theinformation.com/articles/how-tencents-wechat-poses-creeping-threat-to-apple>.

179. *Id.*

180. See *id.* App Store revenue growth in China slowed to 11% in 2019 from triple-digit growth rates in 2015 and 2016. *Id.*

181. See Josh Horwitz, *The Next iPhone Will Mark a Major Test for Apple in China*, QUARTZ (Sept. 11, 2017), <https://qz.com/1073634/the-next-iphone-will-mark-a-major-test-for-apple>.

Given the significance of cross-platform apps, Apple's move to weaken cross-platform apps and favor Apple-unique apps such as Apple Music is particularly problematic. First, Apple's self-preferencing conduct reduces competition between iOS and Android by undermining multihoming apps. For instance, when iOS users are unfamiliar with Spotify's premium services but are fed with push notifications about Apple Music's features, they would know less about Spotify's similar if not superior services available on both iOS and Android. Accordingly, iOS users would have less incentive to switch to Android.

Subscription apps such as Spotify are very important to smartphone owners. About 94% of the top 250 U.S. apps on iOS monetize through in-app subscriptions.¹⁸² The star apps are a critical contributor to user consumption—the top 1% of apps generate 93% of all revenue and 80% of new installs.¹⁸³

Star apps are the few ones that still multihome. For instance, only 8.8% of all iOS apps also exist on Android, while a much higher 47% of apps on the top 100 listings do so.¹⁸⁴ Their multihoming fosters robust smartphone platform competition as consumers would find it easier to switch to alternative platforms with many of the same apps.¹⁸⁵

However, with Apple's increasing exclusionary, self-preferencing conduct, multihoming apps will have a more difficult time competing on iOS even if they are more efficient. Users who already use Apple's apps would face higher costs when switching to alternative providers. This artificial distance created by Apple's self-preferencing conduct thus further locks users within Apple's

in-china (showing 50% retention rate in China); Matt Turner, *UBS Surveyed 8,000 Smartphone Users Around the World, and the Results Should Worry Apple*, BUS. INSIDER (May 28, 2019), <https://markets.businessinsider.com/news/stocks/apple-stock-price-survey-results-should-be-worry-ubs-2019-5-1028236598> (finding the iPhone China retention rate at around 50% and 60% in 2016 and 2019); Rossignol, *supra* note 94 (showing the U.S. retention rate).

182. See Sydow, *supra* note 141.

183. See Williams, *supra* note 142.

184. See Sami Hyrynsalmi, Arho Suominen & Matti Mantymäki, *The Influence of Developer Multi-Homing on Competition Between Software Ecosystems*, 111 J. SYS. & SOFTWARE 119, 123, 123 tbl.2 (2016) (examining app multihoming on App Store's free, paid, and grossing top 100 listings).

185. See Mingchun Sun & Edison Tse, *The Resource-Based View of Competitive Advantage in Two-Sided Markets*, 46 J. MGMT. STUD. 45, 57–61 (2009) (finding reduced competition in single-homing network markets); Jay Pil Choi, *Tying in Two-Sided Markets with Multi-Homing*, 58 J. INDUS. ECON. 607, 625 (2010) (“[T]ying is unambiguously welfare-reducing if multi-homing is *not* allowed.”); *United States v. Microsoft Corp.*, 253 F.3d 34, 53 (D.C. Cir. 2001) (en banc) (finding that if software on Windows is “written for multiple operating systems, its impact could be even greater” as “[t]he more developers could rely upon APIs exposed by such [software], the less expensive porting to different operating systems would be”).

ecosystem and weakens cross-platform competition without necessarily making the consumer experience better.

Second, Apple's conduct slows the rise of new generations of platforms that exist on top of iOS and Android. Facebook's Instant Games platform, which offers mobile games within Facebook, has introduced in-app purchase features for both Android and its web version, but conspicuously not on iOS.¹⁸⁶ Apple's 30% tax is likely a significant factor because when both Facebook and Apple take a cut from game developers' revenue, it becomes harder for developers to profit. Similarly, WeChat's mobile gaming platform generated hundreds of millions of dollars from in-app purchases on Android but has not launched in-app purchase systems on iOS for the explicit reason of the 30% tax.¹⁸⁷ The monetization potential of WeChat's mini-programs is likewise limited. Tencent's guidelines for mini-program developers warn them not to offer digital goods on iOS, but they can provide the goods on Android.¹⁸⁸ This limitation has been a focal point in ongoing negotiations between WeChat and Apple.¹⁸⁹

What these new software platforms and multihoming apps can do is commoditize the iOS platform by creating a new layer of experience independent of the underlying smartphone OS. If users want a WeChat mini-program, a Facebook game instead of a particular iOS app, or multihoming apps such as Spotify, they can find them on both iOS and Android. In many ways, this challenge is similar to Netscape's threat to Windows, where a rising internet browser could commoditize Microsoft's PC operating system monopoly by providing desirable web applications regardless of the underlying OS.¹⁹⁰ To the extent that they limit the rise of future platforms existing on top of iOS, Apple's actions are not unlike what Microsoft did around the turn of the century to prolong its PC operating system monopoly, which the D.C.

186. See Sarah Perez, *In-App Purchases Are Coming to Facebook's Instant Games on Android and the Web*, TECHCRUNCH (May 1, 2018), <https://www.techcrunch.com/2018/05/01/in-app-purchases-are-coming-to-facebooks-instant-games-on-android-and-the-web>.

187. Mengfan Chen, *Special Report | Mini-Programs Facing Battle, Official Accounts Under Pressure—WeChat's Rise and Crises*, CAIXIN WEEKLY (Feb. 25, 2019), <http://weekly.caixin.com/2019-02-23/101382875.html?p0#page2>.

188. See Ma & Osawa, *supra* note 178.

189. See Chen, *supra* note 187.

190. See *Microsoft*, 253 F.3d at 53, 60 (finding that Netscape is the "middleware" that exposes its own APIs (interfaces for third-party developers) and "could take over some or all of Windows's valuable platform functions" which can erode Microsoft's Windows monopoly, as "[a]pplications written to a particular browser's APIs . . . would run on any computer with that browser, regardless of the underlying operating system" and consumers would as a result "no longer feel compelled to select Windows").

Circuit found to constitute illegal monopolization.¹⁹¹ Apple's conduct thus deserves similar antitrust scrutiny and courts should recognize its harm to competition both in the smartphone platform market and the downstream app markets. These harms make Apple's conduct fit under the general monopolization standard,¹⁹² particularly as Apple's proclaimed efficiency justifications ring hollow as Part VII discusses.

VII. HOLLOW EFFICIENCIES AND LESS RESTRICTIVE ALTERNATIVES

Apple may claim its IAP tie and conduct restricting it rivals has procompetitive efficiency justifications, a defense both tying and monopolization cases have considered.¹⁹³ As this Part will show, however, these claimed justifications are either pretextual or not causally necessary and are thus not a sufficient defense.

In considering efficiency justifications, courts often conduct a balancing test that weighs the harm and benefits of the conduct at issue.¹⁹⁴ Given the complexity of balancing two often highly uncertain and complicated effects, however, courts often further employ the Less Restrictive Alternative (LRA)

191. *See id.* at 64, 71–72, 76–78 (finding that a series of Microsoft's restrictive agreements with suppliers and partners to limit Netscape, as well as its actions to undermine non-Microsoft Java virtual machines (another middleware), “represent uses of Microsoft's market power to protect its monopoly” over computer operating systems which “violate § 2 of the Sherman Act”); *see also* Robin Cooper Feldman, *Defensive Leveraging in Antitrust*, 87 GEO. L.J. 2079 (1999) (“Microsoft is leveraging into browsers for one key reason: to prevent browsers from eroding Microsoft's formidable monopoly in the operating systems market.”). Microsoft relied on external partners to limit the distribution of rival browsers and Java virtual machines. *See Microsoft*, 253 F.3d at 60. But Apple can undermine multihoming apps and future platforms on its own thanks to its tight grip on iOS app distribution.

192. *See* text accompanying note 146.

193. *See, e.g.*, *Int'l Salt Co. v. United States*, 332 U.S. 392, 397–98 (1947); *Metrix Warehouse v. Daimler-Benz A.G.*, 828 F.2d 1033, 1035 (4th Cir. 1987); *Breaux Bros. Farms v. Teche Sugar Co.*, 21 F.3d 83, 89 (5th Cir. 1994); *Viamedia, Inc. v. Comcast Corp.*, 951 F.3d 429, 461 (7th Cir. 2020) (supporting a “balancing” test in monopolistic refusal to deal cases).

194. *See, e.g.*, *Eastman Kodak v. Image Tech. Servs.*, 504 U.S. 451, 486 (1992) (leaving as question on remand whether procompetitive effects “outweighed” anticompetitive effects); *Cal. Dental Ass'n v. FTC*, 526 U.S. 756, 771, 774 (1999) (refusing to ignore that gains to competition will outweigh costs from the elimination of across-the board advertising).

test to simplify the calculus.¹⁹⁵ The test asks whether an alternative exists that serves the beneficial goal equally well but with a less anticompetitive effect.¹⁹⁶

A. IAP TIE

Apple proponents have claimed that efficiencies including security, ease of use, app discovery or promotion, app quality control, and general developer support justify Apple's use of the IAP tie.¹⁹⁷ The argument is that if Apple controls the in-app transaction process, it will ensure payment safety and provide a smooth experience; the proceeds from its 30% tax can then be used for promoting third-party apps in the App Store and to support app quality control, development, and distribution. However, applying the balancing and LRA tests shows that these proclamations ring rather hollow.

Some easy balancing for certain key apps exposes the weakness of these claims. To begin with, Apple's promotions are not worth the 30% tax for many big brands like Spotify and Netflix—they are big enough to attract customers themselves without Apple's help. If anything, Apple also benefits from these popular apps in driving demand for the iPhone.¹⁹⁸ In fact, some big app makers have stated they actively do not want Apple's services or other first-party services, if given the choice. For example, Epic Games, the creator of Fortnite, pulled out of the Google Play store and explicitly said it would have done the

195. See C. Scott Hemphill, *Less Restrictive Alternatives in Antitrust Law*, 116 COLUM. L. REV. 927, 937–38, 941, 947–55 (2016) (discussing the difficulty of balancing and how courts often sidestep that question by using the LRA test); *Jefferson Par. Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 25 n.42 (1984) (rejecting “goodwill” defenses in light of less restrictive alternative of using contractual quality specifications); *Fortner Enters., Inc. v. U.S. Steel Corp.*, 394 U.S. 495, 503 (1969) (discussing cases where “tying arrangements generally served no legitimate business purpose that cannot be achieved in some less restrictive way”); *Daimler-Benz A.G.*, 828 F.2d at 1040 (“An asserted business justification cannot salvage a tying arrangement that is otherwise per se unlawful without proof that means less restrictive than the tie-in were not feasible to achieve the desired protection.”).

196. See Hemphill, *supra* note 195, at 937.

197. See *Online Platforms and Market Power, Part 2: Innovation and Entrepreneurship*, Hearing Before H. Judiciary Comm., Subcomm. on Antitrust, Commercial, and Admin. Law (July 16, 2018) (Statement of Kyle Andeer, Apple) (discussing the benefits of the Apple ecosystem, including improved security, ease of use, and integration); Press Release, Apple, Addressing Spotify's Claims (Mar. 14, 2019), <https://www.apple.com/newsroom/2019/03/addressing-spotifys-claims> (discussing the benefits provided by Apple, such as critical software tools and secure payment systems, to Spotify).

198. Apple itself ran a popular ad campaign with the slogan “There’s an app for that.” See Brian X. Chen, *Apple Registers Trademark for “There’s an App for That,”* WIRED (Oct. 11, 2010), <https://www.wired.com/2010/10/app-for-that>.

same for the iOS version of the battle royale game but for Apple's restrictions on installation of apps from third-party sources.¹⁹⁹

These supposed efficiency justifications crumble further in the face of three LRAs. First, Apple would actually profit more from offering lower fees to the big apps, and that it has not done so suggests ill intent implying likely anticompetitive effect. Netflix, for example, generated \$853 million in 2018 revenue on iOS before it pulled out of IAP, which means Apple's 30% take from Netflix alone was around \$256 million in that one year.²⁰⁰ For Apple to offer a more acceptable 10% rate and get 10% of \$853 million would be much better than getting 30% of nothing when these apps pull out.²⁰¹ But Apple has chosen to forgo these enormous profits, which suggests it is expecting even more gains from restraining these apps.

Second, the claimed quality control, security, developer support, and promotional efficiencies are not causally related to the IAP tie and the 30% tax, and they likely would have been provided regardless. To protect iPhone's deliberately cultivated status as a premium brand, Apple would hardly allow its apps' quality control or security to slip. Indeed, Apple's own Mac computer does not tie its app-purchase system to digital goods distribution, but it is still secure and has decent quality control by Apple's own account.²⁰² Similarly, Apple offered quality control, developer support, and app promotions to subscription apps before it imposed the 30% tax and IAP on them in 2011.²⁰³ Furthermore, broad-based developer support is a sine qua non for all successful modern software platforms, and such support is routinely offered without an expensive 30% tax.²⁰⁴ In fact, Apple already charges a \$99 annual

199. See Liz Lanier, *'Fortnite' Avoiding Google Play Store's 30% Cut on Android Version*, VARIETY (Aug. 4, 2018), <https://www.variety.com/2018/gaming/news/fortnite-avoiding-google-play-stores-30-cut-on-android-version-1202895335>. Epic was eventually removed from the iOS App Store in August 2020 after refusing to pay Apple's 30% tax. See Hollister, *supra* note 106.

200. Sarah Perez, *Netflix Stops Paying the 'Apple Tax' on Its \$853M in Annual iOS Revenue*, TECHCRUNCH (Dec. 31, 2018), <https://www.techcrunch.com/2018/12/31/netflix-stops-paying-the-apple-tax-on-its-853m-in-annual-ios-revenue>.

201. An argument can be made that perhaps Apple should pay these big apps rather than the reverse, as Apple can get more revenue from the increased demand for the iPhone generated by these popular apps.

202. See *Security. Built Right In.*, APPLE, <https://www.apple.com/macOS/security> (last visited Jan. 4, 2021) (touting Mac apps' security).

203. See text accompanying note 124.

204. See MICROSOFT DEVELOPER, <https://developer.microsoft.com/en-us> (offering support tools); Microsoft Store Team, *A New Microsoft Store Revenue Share Is Coming*, WINDOWS BLOGS (May 7, 2018), <https://blogs.windows.com/windowsdeveloper/2018/05/07/a-new-microsoft-store-revenue-share-is-coming> (charging a mere 5%).

developer fee for support tools needed to develop, test, and distribute apps.²⁰⁵ Finally, promotions are also independently provided through Apple's Search Ads program. This program advertises apps for a fee when users conduct searches and is expected to generate \$2 billion in 2020.²⁰⁶ It is thus disingenuous to say that without the 30% fee Apple would not be able to provide these efficiencies.

Third, if Apple's IAP provides clear security and ease of use benefits, users and developers will adopt it as a matter of choice. As the Fourth Circuit has held, if security is the concern, the tying firm "could have required its dealers [or developers in Apple's case] to inform their customers" of the alternative payment mechanism developers offer and their associated security risks (as Apple already does with Mac apps from third-party sources).²⁰⁷ Citing the Supreme Court, the court observed that "any intrinsic superiority of the 'tied' product would convince freely choosing buyers to select it over others, anyway. Perceived consumer expectation, without more, will rarely justify an unlawful tie-in."²⁰⁸ This unchosen LRA based on information and buyer choice, rather than a forced tie, offers much of the same benefit claimed and is much less restrictive. No efficiency justification here can therefore outweigh the significant harm the IAP tie creates.

B. IMPAIRING RIVALS

Many of Apple's other practices impairing rivals and favoring its proprietary apps may have potential efficiencies related to quality control, privacy, and integration, but they can again be achieved through less restrictive alternatives. Apple may claim, for example, that restricting third-party apps' notification-based promotions, access to user data, NFC, and certain other iPhone features may improve user experience and security.²⁰⁹ As noted above, quality control is not a justification if a less restrictive means exists to ensure quality, such as specifying standards.²¹⁰ Apple can thus simply require third-party apps to meet certain quality standards for promotions or data and NFC access instead of banning these apps outright. This alternative is often viable

205. See *Membership Details*, APPLE DEVELOPER PROGRAM, <https://developer.apple.com/programs/whats-included> (last visited Jan. 4, 2021).

206. See Lauren Feiner, *Apple's App Store Ads Could Be a \$2 Billion Business by 2020*, *Bernstein Analyst Predicts*, CNBC (Oct. 22, 2018), <https://www.cnbc.com/2018/10/22/apple-app-store-ads-to-be-2-billion-business-by-2020.html>.

207. *Metrix Warehouse v. Daimler-Benz A.G.*, 828 F.2d 1033, 1041 (4th Cir. 1987).

208. *Id.* (internal quotation marks omitted) (citing *Times-Picayune Publishing Co. v. United States*, 345 U.S. 594, 605 (1953)).

209. See, e.g., Slivka, *supra* note 155.

210. See text accompanying notes 207–208.

as evidenced by the parental control app incident.²¹¹ Similarly, if prominent promotions for Apple's apps help launch desirable products, similar openings should be available to third-party developers (e.g., by auction) who will pay for such services to the extent their apps are valued by users and thus profitable.

Apple can also offer users information and choice that will allow them to decide for themselves whether they desire certain claimed benefits. For example, Apple could allow users to turn off Apple's promotions for its proprietary apps as well as those from third-party apps instead of forcing Apple's ads while prohibiting third-party promotions; or Apple could also ask users for permission before sending Apple ads when Apple already requires other apps to do so.

Discriminatory access to certain private APIs presents a trickier issue. Opening iPhone's NFC and Siri features to third-party apps may require Apple to create and maintain certain protocol outside access, which may involve non-trivial technical costs. This burden may justify a slightly delayed rollout for third-party support. However, the benefits from competition that incentivize developers to offer better deals and more choices to consumers as a result of opening access may significantly outweigh the non-negligible but not prohibitive cost of creating public APIs for key features such as Siri and NFC. As access to voice control is quite important for music apps and NFC is essential for modern proximity payment apps, the competitive harm from not opening access likely dominates over the technical costs.

Either Apple's restrictions on third parties are not causally necessary to the claimed benefits or substantially less restrictive alternatives exist. As a result, Apple's claimed efficiencies provide no sufficient defense for the significant harm of its exclusionary conduct. Apple has therefore abused its dominance to force the IAP tie and expand its monopoly in the smartphone platform market. The fortress of its walled garden keeps out not only competition but also innovations that could transform the future of technology, to the detriment of the entire digital economy and hundreds of millions of consumers. Accordingly, Apple's conduct violates antitrust law for illegal tying and monopolization.

Current judicial doctrines on monopoly leveraging and refusal to deal, however, may impede enforcement against platforms' abuse of dominance. Antitrust law thus needs new tools to contain the rise of consumer platform abuses in the twenty-first century.

211. See text accompanying notes 154–158.

VIII. ANTITRUST FOR THE 21ST CENTURY

As Parts IV-VII have shown, Apple has leveraged its dominance to expand its mobile platform monopoly, harming competition and consumers. Its conduct should therefore be condemned under antitrust law's general monopolization standard. Yet courts often follow precedents on specific exclusionary conduct with a restrictive reading of what constitutes monopolization. Monopoly leveraging and refusal to deal doctrines, for example, put a high burden of proof on plaintiffs to show exclusionary outcomes as discussed in Part II.²¹² This judicial reluctance to recognize exclusionary conduct may even spill over to tying claims that resemble refusal to deal, letting otherwise illegal tying pass under judicial watch. This Part exposes the misplaced assumptions behind these doctrines and calls for a doctrinal reform.

A. RECONSIDER LEVERAGING

When platform operators such as Apple leverage their power to restrict downstream markets on a platform through exclusion and discriminatory treatment of rivals, significant competitive distortions and consumer welfare losses can result as shown in Parts V and VI. Relying on the "one monopoly profit" theory as discussed in Part II, however, the current leveraging doctrine requires dangerous probability of monopolization in downstream markets to prove illegality, despite significant harm from expanded monopoly even short of achieving monopoly power in these secondary markets.²¹³

Apple's example pokes a conspicuous hole in the Chicago School's theory of benign leveraging embraced by courts today.²¹⁴ The "one monopoly profit" theory courts rely on rests on special assumptions that do not hold true for platform markets. It ignores transaction costs and assumes static market competitiveness²¹⁵ and rational actors. As Parts III-VII have documented, significant information costs from limited consumer and small business resources and capabilities mean that buyers in platform markets systematically do not take secondary market prices into full account;²¹⁶ strong lock-ins across product ecosystems prevent platform users and partners to switch away even when they become aware of supracompetitive prices;²¹⁷ and the temptation of

212. See *supra* text accompanying notes 36–48.

213. See *supra* text accompanying notes 36–42.

214. See *supra* text accompanying notes 34–42.

215. See Einer Elhauge, *Tying, Bundled Discounts, and the Death of the Single Monopoly Profit Theory*, 123 HARV. L. REV. 397, 413–19 (2009).

216. See *supra* Sections III.A–B, IV.B–C.

217. See *supra* Sections III.C, IV.B–C.

successive monopolies and network effects in both upstream and downstream markets incentivize dominant firms to employ even inefficient leveraging to preserve and expand their profitable dominance.²¹⁸ As a result, iPhone users have to pay supracompetitive prices for both the iPhone and many key apps as well as tolerate experience and innovation losses without the practical ability to switch away to more efficient choices when Apple leverages its power downstream.²¹⁹ Although Apple could indeed monopolize certain markets with its totalizing control such as in contactless proximity payment and parental control markets, the competitive harm of its conduct does not depend on its monopoly status downstream but rather upstream—as shown by damages in many other markets (e.g., streaming music) even without such complete exclusion.²²⁰

Courts should thus recognize leveraging's exclusionary effect when there are significant information and switching costs and strong network effects. Accordingly, they should reestablish monopoly leveraging as an independent category of exclusionary conduct that can violate Section 2 of the Sherman Act without necessarily requiring a dangerous probability of monopolization of the second market, as they did before the Chicago School era.²²¹ Courts should also jettison the associated burdensome and unnecessary market definition requirement for downstream markets affected by leveraging.²²² Courts should allow plaintiffs to focus on proving actual harm as long as such harm is substantial enough (e.g., worth over a monetary threshold such as \$10 million). Such reform will better address the often very significant harm from platform monopolists that escapes the ambit of current Section 2 doctrines.

In administering the new leveraging doctrine, an LRA-based approach may help limit overly expansive enforcement that could discourage efficient leveraging. While monopoly leveraging can have significant harms as Part VI demonstrates, it is possible to have certain efficient vertical integration. For example, Apple may better coordinate internally about what software features to adopt for a new phone, which might benefit both Apple's apps and third-party apps. If the new features make Apple's apps work better without making third-party apps function worse, such leveraging should be preserved. The LRA-based approach preserves bona fide efficiencies when no equally

218. See *supra* Sections III.D, IV.A, VI.A; Feldman, *supra* note 191; Whinston, *supra* note 76; Brian, *supra* note 76; Carlton & Waldman, *supra* note 76.

219. See *supra* Sections IV.B-C, V.B, VI.A.

220. See *supra* Sections VI.A-B.

221. See *United States v. Griffith*, 334 U.S. 100, 107–09 (1948); *United States v. Paramount Pictures*, 334 U.S. 131, 174 (1948).

222. See *supra* text accompanying notes 37–40.

effective and less restrictive alternatives exist, while screening out pretextual efficiencies and unnecessary restrictions.²²³

B. RATIONALIZE THE REFUSAL TO DEAL DOCTRINE

Similar to the flawed leveraging doctrine, courts should reconsider their narrow interpretation of the refusal to deal doctrine.²²⁴ Apple's exclusion and discriminatory treatment of rival apps entail "unreasonable terms and conditions" that constitute effective refusal to deal.²²⁵ Courts, however, have singularly focused on ending a prior course of dealing as the requirement for illegal refusal to deal.²²⁶ With the changing dynamics of platform markets, judges should be less rigid in recognizing alternative reasons for illegal refusal to deal—in particular, platforms' role as the essential infrastructure of the modern digital economy and the dangers of installed-base opportunism.

First, platforms' role as today's essential digital infrastructure further cautions against judicial hostility to refusal to deal claims. Current literature has extensively documented the infrastructural nature of tech platforms as computer and smartphone operating systems, cultural and political public forums, and e-commerce platforms, finding strong positive spillovers from their open access.²²⁷ Platforms' essential role in combating COVID-19 recently has underscored their social importance.²²⁸ The positive externalities from their openness mean restricting access to key platforms, such as Apple's

223. See *supra* Part VII.

224. See *supra* text accompanying notes 45–48.

225. See *MetroNet Servs. Corp. v. Qwest Corp.*, 383 F.3d 1124, 1132 (9th Cir. 2004) (holding terms that “would not be profitable for the plaintiff [or competitor to the monopolist defendant] to accept” was a “practical refusal to deal”).

226. See *supra* text accompanying notes 45–48.

227. See Geoffrey Parker, Marshall Van Alstyne & Xiaoyue Jiang, *Platform Ecosystems: How Developers Invert the Firm*, 41 MGMT. INFO. SYS. Q. 255 (2017) (showing that open access is more advantageous than closed organization for platform firms such as Apple, Google, and Microsoft, with significant knowledge spillovers); Brett Frischmann & Spencer Weber Waller, *Revitalizing Essential Facilities*, 75 ANTITRUST L.J. 1, 55 (2008) (finding that Microsoft's Windows operating system's “downstream externalities for both software developers and individual computer users are both immense and incalculable”); Frank Pasquale, *Dominant Search Engines: An Essential Cultural & Political Facility*, in *THE NEXT DIGITAL DECADE* 401 (Berin Szoka & Adam Marcus eds., 2011); Jean-Christophe Plantin, Carl Lagoze, Paul N. Edwards & Christian Sandvig, *Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook*, 20 NEW MEDIA & SOC'Y 293 (2016); Zachary Abrahamson, Comment, *Essential Data*, 124 YALE L.J. 867, 879 (2014); Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 802 (2017).

228. See, e.g., Brian Fung, *The Pandemic Is Playing to Almost Every One of Amazon's Strengths*, CNN (Apr. 9, 2020), <https://www.cnn.com/2020/04/09/tech/amazon-dominance-coronavirus> (“As the coronavirus pandemic has forced people to stay inside, few companies have proven themselves as essential as Amazon.”).

smartphone ecosystem, has negative consequences beyond what is incorporated in their private profitability calculations.

Antitrust law's essential facilities doctrine, now dormant but once active in the era of deregulation, in many ways represents courts' recognition of the social importance of maintaining reasonable access to essential infrastructure.²²⁹ As such infrastructure facilities derive the bulk of their social value from downstream innovations—for example, by the millions of apps on iPhone rather than the metal bar itself and its basic software framework—courts have required them to open access to downstream market players who might compete with the owner of the infrastructural input to facilitate social innovations.²³⁰ Following this history, courts today should also take into account the infrastructural nature of tech platforms and reconsider the risk of their refusal to deal.

Second, Apple's discriminatory treatment of rivals on its platform serves as an example of installed-base opportunism and militates against the rigid refusal to deal doctrine. When the App Store was launched in 2008, subscription-based third-party apps were free to choose their own payment methods, including non-IAP alternatives.²³¹ Developers arrived in droves to create hundreds of millions of apps for the iPhone, a critical factor in iPhone's success.²³² In 2011, however, Apple limited subscription apps' payment choice to Apple's own IAP system which requires a 30% tax.²³³ This move hurt developers' businesses and started a trend where Apple increasingly tries to capture the benefits of the platform for its own profits rather than for the developers who have created the hundreds of millions of apps that attract users.

229. See Frischmann & Waller, *supra* note 227, at 8, 10–17.

230. Courts have applied the essential facilities doctrine to infrastructure such as railroad bridge, power utility, and telephone networks. See *United States v. Terminal R.R. Ass'n of St. Louis*, 224 U.S. 383, 411–13 (1912); *Otter Tail Power Co. v. United States*, 410 U.S. 366, 380–83 (1973); *MCI Comm'ns Corp. v. AT&T Co.*, 708 F.2d 1081, 1132–33 (7th Cir. 1983).

231. See TREEHOUSE, *supra* note 124 (“Apple just dropped a nuclear bomb on all of us Apple will not allow you to encourage your iOS customers to pay for your subscription service outside the App Store fence.”).

232. See Garcia-Swartz & Garcia-Vicente, *supra* note 72, at 883, 889 (finding that “the iPhone did not really take off before the opening of the App Store” and that each extra app by developers is associated with 271–386 additional users). Apple itself also admitted the importance of developers: “[i]f third-party software applications and services cease to be developed and maintained for the Company's products, customers may choose not to buy the Company's products.” Apple Inc., Annual Report (Form 10-K) (Oct. 30, 2020), <https://sec.report/Document/0000320193-19-000119>.

233. See TREEHOUSE, *supra* note 124; Gruber, *supra* note 124.

In the early days of the App Store, Apple also had little presence in the subscription app market. Given the uncertainty of what was a whole new platform, developers reasonably did not fully expect that Apple would later enter this market and compete directly with them in such a sweeping fashion as it does now,²³⁴ often using its power as the App Store gatekeeper to disadvantage rivals and tip the competitive balance in its own favor. Apple's discriminatory treatment of Spotify, a competitor to its Apple Music app in the streaming music market as detailed in Sections V.B and VI.A, is an emblematic example of such a trend. In all these cases, third-party app developers have played a crucial role in the success of the Apple ecosystem but are now expropriated by Apple who imposes its power to claim more than its fair share of the platform proceeds.

Apple's conduct further threatens the platform economy's long-term sustainability. Allowing Apple to abuse the system and expropriate third-party developers can deter the investment of future developers and potential participants in other platforms. Knowing that platforms will exploit them, platform participants are less likely to invest in the platform in the first place. Professor Carl Shapiro has spoken about this phenomenon which he terms "installed-base opportunism":

[I]n a network industry, a firm might obtain a dominant position based in part on certain "open" policies that induce reliance by complementary firms, and then later exploit that position by offering less favorable interconnection terms or by refusing to interconnect with them altogether [F]ear of opportunism can dull the incentives of other parties—downstream firms, suppliers of complements, rival networks, or final customers—to make investments.²³⁵

Apple's relatively early openness and its growing self-preferencing intervention in downstream app markets similarly risk reducing future investments in the platform. As a result, if Apple's conduct is allowed, iPhone users would increasingly experience fewer and less impactful innovations on the platform as developers shy away, a net loss for consumer welfare.

If this kind of self-preferencing is allowed with impunity, platforms in general will see less investment from third parties who fear ex post expropriation. Despite their many flawed practices, tech platforms have also in many ways been engines of innovation, creating millions of jobs and

234. See *supra* text accompanying notes 17–20.

235. CARL SHAPIRO, EXCLUSIONARY CONDUCT: TESTIMONY BEFORE THE ANTITRUST MODERNIZATION COMMISSION, ANTITRUST MODERNIZATION COMMISSION 15–16 (2005), <https://faculty.haas.berkeley.edu/Shapiro/amcexclusion.pdf>.

providing significant consumer benefits. However, without the active and often passionate participation of third-party app developers, merchants, news publishers, and other players, these platforms would not have been able to achieve all these welfare improvements. As potential platform participants grow wary, future platforms will find it harder to grow their ecosystems and drive innovation. The net result will be a loss of productivity growth and consumer welfare on an economy-wide level and particularly in innovative markets where platforms tend to provide unique value.

Ultimately, monopolists' prior dealing should serve only as a heuristic—a useful evidentiary device, but not the sole determinant of illegal refusal to deal. If a party abruptly ends a voluntary and thus likely profitable contract, it often suggests some ill intent behind the move to hurt competitors. However, many other refusal scenarios can have exclusionary effects,²³⁶ as this Part has shown. Narrowly focusing on but one cause of anticompetitive harm in refusal to deal cases, as courts do now, will only cause them to overlook damaging exclusionary conduct that will likely be increasingly common by tech platforms in multilayered network markets that provide strong incentives for refusal to deal everywhere. Worse, such judicial reluctance to recognize anticompetitive refusal to deal may even spill over to tying claims that resemble refusal to deal.²³⁷ As the remedy for illegal tying is to untie a forced combination of transactions, it often means requiring the antitrust defendant to be more open and deal with third parties—non-Apple payment systems on iOS, for example. Judges hostile to refusal to deal claims may very well let such anticompetitive tying pass,²³⁸ which would otherwise be illegal under current case law on tying. Doing so would leave consumers vulnerable to anticompetitive harm.²³⁹

Courts should thus unanchor the refusal to deal doctrine from the prior dealing requirement, at least for tech platforms, when refusal to deal excludes competitors despite the presence of LRAs, as the Seventh Circuit recently hinted.²⁴⁰ One concern about refusal to deal remedies is that specifying the

236. See generally Adam Candeub, *Trinko and Re-Grounding the Refusal to Deal Doctrine*, 66 U. PITT. L. REV. 821 (2005).

237. See 3B AREEDA & HOVENKAMP, *supra* note 81, ¶ 772 (“Refusals to deal in dominated, path-dependent networks . . . can resemble tying arrangements.”).

238. See *id.* (stating that current law on refusal to deal is “overinclusive” as judges consider refusal to deal “virtually per se lawful”).

239. See *supra* Section V.B.

240. See *Viamedia, Inc. v. Comcast Corp.*, 951 F.3d 429, 463 (7th Cir. 2020) (“We leave open the question whether allegations of short-term losses are necessary [O]ther factors—such as a prior course of conduct, exploitation of power over a cooperative network, refusal to sell at retail price, and discriminatory treatment of rivals—could plausibly support the inference that a refusal to deal is prompted . . . by anticompetitive malice.” (internal citation and quotation marks omitted)).

terms of the required deal may turn judges into regulators, who may not be in the best position to dictate what constitute efficient terms.²⁴¹ Using LRAs as a basic approach for providing refusal to deal remedies, however, can allow plaintiffs to put forth specific alternatives which can achieve similar efficiencies with less restrictive means, as Part VII has demonstrated. This would alleviate the courts' job because they would only need to evaluate specific alternative scenarios already provided and their marginal benefits over the status quo instead of having to compare the aggregate balance of harm and benefits and devise a comprehensive scheme of remedy.²⁴²

C. RECALIBRATE ENFORCEMENT: CLASS CERTIFICATION AND PRIVATE-PUBLIC DIVISION OF LABOR

U.S. antitrust law can be enforced by either private litigants or government agencies such as the FTC and DOJ. This dual-track system often gives different roles to private parties and the enforcement agencies in upholding antitrust law due to their different capabilities and strengths. The consumer platform economy today has brought about important changes to market dynamics and the need to reimagine antitrust law. These shifts require a careful recalibration of antitrust enforcement laws and the division of labor between private and public enforcers to bring the new antitrust regime to reality.

This Section explores (1) the difficulties of private class actions against dominant consumer platforms and the importance of permissive class certification standards, which are critical for ensuring the viability of private antitrust enforcement, and (2) the need for expanding public enforcement as well as new agency priorities (especially investigating possible LRAs, expanding current doctrines, and enforcement on behalf of small players) in the age of consumer platforms.

1. *Private Class Actions*

Class actions play a vital role in the private enforcement of U.S. antitrust law thanks to their role in “aggregating large numbers of small claims, which otherwise would [be] nearly impossible to litigate on an individual basis.”²⁴³ In

241. See *Verizon Commc'ns v. Law Offs. of Curtis V. Trinko, LLP*, 540 U.S. 398, 407 (2004); Herbert Hovenkamp, *The Reckoning of Post-Chicago Antitrust*, in POST-CHICAGO DEVELOPMENTS IN ANTITRUST LAW 11 (2002).

242. Cf. James A. Henderson Jr. & Aaron D. Twerski, *Achieving Consensus on Defective Product Design*, 83 CORNELL L. REV. 867, 884–85 (1998) (discussing similar virtues of tort law's Reasonable Alternative Design doctrine); see also HOVENKAMP, *supra* note 35, at 395, 415 (concluding that antitrust provides a more modest form of regulation for dominant network firms than utility regulations).

243. Spencer Weber Waller & Olivia Popal, *The Fall and Rise of the Antitrust Class Action*, 39 WORLD COMPETITION 29, 29 (2016).

doing so, private enforcement generates deterrence “by multiplying the total resources committed to the detection and prosecution” of antitrust violations.²⁴⁴ The Supreme Court has also recognized that “private enforcement . . . provides a necessary supplement” to public enforcement given the latter’s limited resources.²⁴⁵

In reality, however, class actions in general often do not live up to their promise, principally due to agency problems. Because class attorneys are “unconstrained by the dictates or interests of a specific client,” four important factors misalign their incentives with plaintiffs’ and in turn the goal of private antitrust law: (1) risk aversion as the attorney is more invested in the litigation, has more to lose, and thus is more willing to settle early often for inadequate amounts; (2) collusion between attorney and defendant that produces a lower settlement amount but higher attorney fees; (3) lack of property rights in the litigation so that other attorneys can join and reduce the award to each attorney; and (4) greater search costs compared to non-class litigations, as the class attorney cannot get much information from his clients due to their tenuous attorney-client nexus and would thus need to “play private detective.”²⁴⁶

Class actions against dominant consumer platforms face further difficulties. First, search costs are even greater in these cases. The hundreds of millions of individual consumers and small businesses (e.g., app developers) on a platform usually have even less information about the defendant than traditional antitrust plaintiffs. These plaintiffs mostly consist of the defendant’s competitors or downstream businesses suing their suppliers²⁴⁷ that tend to be more sophisticated firms and deal with the defendant on a closer basis than the fragmented platform participants today which only deal with tiny parts of a giant platform.

Second, the diverse demand and supply dynamics of a broad-based consumer platform pose significant challenges to class certification, in turn chilling plaintiffs’ and attorneys’ incentives to pursue lawsuits. To bring a class action and claim damages as compensation, plaintiffs must first certify as a class by meeting certain requirements. These requirements include predominance under Civil Procedure Rule 23(b)(3), which says “questions of

244. John C. Coffee Jr., *Rescuing the Private Attorney General: Why the Model of the Lawyer as Bounty Hunter Is Not Working*, 42 MD. L. REV. 215, 218 (1983).

245. *J.I. Case Co. v. Borak*, 377 U.S. 426, 432 (1964).

246. Coffee, *supra* note 244, at 229–34.

247. See Paul V. Teplitz, *The Georgetown Project: An Overview of the Data Set and Its Collection*, in PRIVATE ANTITRUST LITIGATION 68 (Lawrence J. White ed., 1988).

law or fact common to class members predominate over any questions affecting only individual members.”²⁴⁸

Predominance for the question of damages can be particularly fraught for consumer-platform plaintiffs. To prove common questions of damages, plaintiffs often must offer a model that can calculate classwide damages susceptible to common evidence.²⁴⁹ However, dominant platforms’ anticompetitive conduct often span the multitude of their products and services, targeting very different groups and causing harms to different degrees. For example, Apple’s exclusionary conduct happens across its IAP tie, its limits on third-party access to NFC and Siri, and its self-preferencing over push-notification advertising, affecting developers and consumers in different markets.²⁵⁰ A complete absence of alternative NFC payment apps and suppressed innovation in the streaming music market due to Apple’s restrictions on rivals’ promotions likely result in divergent consumer losses, which would need different evidence to calculate. Moreover, heterogeneous supply and demand on a broad-based platform means even the same conduct may have divergent impacts on different groups. While Apple’s 30% tax is consistent across apps, developers who have different levels of profit margins may act differently in the alternative world with an LRA of, say, 5% Apple tax for optional IAP usage—some may choose the IAP system for secure transaction processing; some might not if their margins are too low.

As the existence of individual conduct impacts supply and demand factors and precludes the exclusive use of common evidence for a model that estimates damages reliably, the diversity in the degree of anticompetitive harm across groups may thus impede certification of a class that includes all platform participants. But without forming a class, small individual plaintiffs (and their lawyers) have little incentive to bring an expensive lawsuit just to recover a small amount of individual damages, effectively defeating private antitrust enforcement.

A heightened pleading standard in recent case law further complicates class certification. Traditionally, courts have certified classes even if individual questions of damages predominate over common ones, as long as antitrust liability still presents common issues—that is, as long as plaintiffs can use common evidence to prove antitrust violations, they can proceed as a class to prove liability first and then determine damages individually afterwards.²⁵¹

248. See AM. BAR ASSOC., 1 ANTITRUST LAW DEVELOPMENTS 836 (8th ed. 2017).

249. See *Comcast Corp. v. Behrend*, 569 U.S. 27, 34 (2013); Paul A. Johnson, *The Economics of Common Impact in Antitrust Class Certification*, 77 ANTITRUST L.J. 533 (2011).

250. See *supra* Sections III.A, IV.B.

251. See 1 ANTITRUST LAW DEVELOPMENTS, *supra* note 248, at 837.

However, after the Supreme Court in a 5–4 decision instructed courts to “probe behind the pleadings before coming to rest on the certification question” to meet predominance standards,²⁵² some lower courts have been closely examining even *damages* at the certification stage to determine whether they form questions common to the class and have denied certification if they do not.²⁵³ This recent development thus frustrates class actions at an earlier stage and further chills private incentives to police antitrust violations.

Fortunately for antitrust plaintiffs, this recent line of cases has not dominated in all courts, and a circuit split currently exists over whether common questions regarding damages are necessary for class certification.²⁵⁴ There is a strong argument that they should not be necessary, especially for consumer platform plaintiffs.

First, the drafters of the Civil Procedure rules explicitly stated that it is “an appealing situation for a class action . . . despite the need, if liability is found, for separate determination of the damages suffered by individuals within the class,” signaling the intent of the rule.²⁵⁵ Second, “the predominance requirement calls only for predominance, not exclusivity, of common questions” as some courts have noted.²⁵⁶ As long as liability, the main question in an antitrust case, presents common questions rather than individual ones, the class action will be mostly based on common issues. Third, Civil Procedure Rule 23(c)(4) directs that “an action may be brought or maintained as a class action with respect to particular issues.”²⁵⁷ Courts may thus certify a class in which only certain but not all issues in the underlying controversy are to be resolved collectively.²⁵⁸

These class certification rules that allow separate adjudications for liability and damages are particularly important for consumer platform plaintiffs. These plaintiffs already face special difficulties over common issues of damages. If certification is simply banned over individualized questions of damages, consumer platform antitrust class actions would effectively be

252. *Comcast*, 569 U.S. at 33.

253. See Elena Kamenir, *Seeking Antitrust Class Certification: The Role of Individual Damage Calculations in Meeting Class Action Predominance Requirements*, 23 GEO. MASON L. REV. 199, 200 (2015).

254. See *id.* at 214–16.

255. See *id.* at 220; Amendments to Rules of Civil Procedure, Supplemental Rules for Certain Admiralty and Maritime Claims, Rules of Criminal Procedure, 39 F.R.D. 69, 103 (1966).

256. E.g., *Shelter Realty Corp. v. Allied Maintenance Corp.*, 75 F.R.D. 34, 37 (S.D.N.Y. 1977).

257. FED. R. CIV. P. 23.

258. See Kamenir, *supra* note 253, at 262.

foreclosed despite having predominantly common underlying questions of antitrust liability. The supposed alternative—individual actions—is practically impossible for most platform monopoly victims given their numerosity and lack of financial resources to afford a protracted legal fight against lavishly funded tech giants. It is thus critical to separate class certification from questions of damages at least at the initial stage of the lawsuit.

Two other class certification principles that correctly interpret “predominance” as actual predominance as opposed to exclusivity are also important for courts to adopt in consumer-platform class actions. If a question fails to affect every class member, it does not mean that it affects “only individual [class] members.”²⁵⁹ Instead of this dichotomy, there is a continuum between questions common to all class members and those specific to only individual members. Along this continuum are issues common to important subgroups of the class. For example, the anticompetitive effect of Apple’s self-preferencing conduct in the streaming music app market is an issue common to all streaming music users on iOS. Such users constitute an important subgroup of the iPhone user class given their likely significant representation in a consumer platform class action against Apple. Yet the effect of Apple’s conduct in this market is not an issue common to non-music listeners in the class. The same goes for the issue of NFC foreclosure to mobile payment users. As long as the relevant subgroups are important enough for issues common to them to collectively predominate truly individualized issues, class certification should be granted. As such industry subgroups affected by platform abuse of dominance are likely common, this interpretation of the predominance element will be important to preserve incentive for private enforcement against dominant platforms.

Second, class certification should not be denied just because some class members are not injured. Given the enormous number of platform users, there will probably be a small number of them who have not purchased any apps and may not have purchased any even absent anticompetitive behavior. With the enormous scale of today’s consumer platforms, however, even a small percentage of uninjured users may seem large in absolute terms. It is thus important not to deny certification based merely on this small number of users; otherwise it would similarly preclude class actions against platforms in effect.

While both principles may seem sensible if not obvious, some courts unfortunately do not adopt them or do not consistently do so despite many of their peers’ acceptance.²⁶⁰ It is therefore worth reiterating the importance of

259. See J. Douglas Richards & Benjamin D. Brown, *Predominance of Common Questions—Common Mistakes in Applying the Class Action Standard*, 41 RUTGERS L.J. 163, 178–81 (2009).

260. See *id.* at 173–81.

these principles particularly in today's consumer platform economy, where private actions will often be effectively foreclosed by a contrary policy.

Perhaps a more radical proposal for easing class certification is to allow averaging impact to satisfy the commonality requirement for certain parts of damages. For example, to produce a class for the purpose of overall damages determination, cases can aggregate and average diverse damages for app developers who may pay different rates for in-app transaction processing in an alternative scenario without a forced IAP and 30% tax. This can again ease the litigation burden for each small developer who would otherwise need to bring the suit or participate in the damages proceeding independently. As each would need to hire their own expensive lawyers which may eat up much of the litigation award,²⁶¹ a rule prohibiting average impact may again effectively eliminate private actions.

In fact, a Supreme Court class certification case already permitted statistical averaging. In *Tyson Foods v. Bouaphakeo*, plaintiffs averaged workers' production times to demonstrate predominance of common questions.²⁶² While the Court refused to promulgate any general rules apart from the specific facts of the case, it can be a sensible rule when averaging is possible and not far from the actual damages for a class. It would remove a major obstacle to private enforcement of antitrust violations by offering more proportionate incentives for class attorneys, reduce their risk aversion, and better align attorney and plaintiff incentives.

2. Public Enforcement

A public-private partnership in antitrust enforcement offers a useful baseline to determine the role of agencies and identify their priorities in enforcing antitrust law in today's consumer platform economy. John Coffee has observed a model of antitrust public enforcement that focuses on detection with its investigative resources, works on cases likely to generate publicity and political visibility, and breaks new legal ground and sets legal precedents, but is less interested in the financial damages recoverable.²⁶³ Private plaintiffs, on the other hand, piggyback on successful agency actions to recover damages with their greater experience in litigation, offering greater and often more proportionate deterrence beyond "the modest [agency] fine

261. On average, 60% of an antitrust award can go to litigation costs. See Ira M. Millstein, *The Georgetown Study of Private Antitrust Litigations: Some Policy Implications*, in PRIVATE ANTITRUST LITIGATION 399, 402 (Lawrence J. White ed., 1988). Distribution of an award amongst developers can be determined after the proceeding through negotiations. So averaging the damages for certification purposes does not necessarily mean equally distributing the award.

262. See 136 S. Ct. 1036, 1049 (2016).

263. See Coffee, *supra* note 244, at 228, 228 n.28.

schedules that are authorized by law”—which top at \$1 million for a corporation whereas private damages or settlement amounts can reach billions of dollars.²⁶⁴ Given this public-private enforcement dynamic, enforcement agencies should be more active overall to provide evidence, explore specific LRAs, expand leveraging and refusal to deal doctrines, and pay particular attention to small players.

First, agencies need to be more active in bringing lawsuits against dominant consumer platforms to provide evidence. Three factors underincentivize consumer platform class attorneys even more than usual to obtain information and to bring enough suits: (1) the significant search costs for private class actions overall, (2) currently stringent class certification standards for damages that pose special difficulties to platforms, and (3) the complexity of platform market power and the dynamic mechanisms of harm. Although agencies are already investigating major tech platforms, they should be more aggressive in bringing actions or otherwise issuing public reports detailing their findings, which can help private enforcement with information from investigations. To aid this expansion, Congress should provide more resources to the DOJ and FTC antitrust divisions by providing bigger budgets, more personnel, and private market-competitive salary as commentators have argued.²⁶⁵

Second, agencies should actively explore possible LRAs to anticompetitive conduct using their greater investigate resources. LRA proposals can be extremely fact-intensive, as Sections III.D and IV.C have demonstrated, making them unsuitable for private class actions which lack information. The current underuse of LRAs may well be a result of under-pleading by plaintiffs. With agencies leading the charge on evidence-finding that demonstrates LRAs, they can be enormously helpful in establishing liability for consumer platforms in what can otherwise be very tough balancing acts.²⁶⁶

Third, agencies should try to expand the boundaries of antitrust law for consumer platforms. In particular, they should expand monopolistic leveraging and refusal to deal doctrines as argued in Section V.A, using their freedom to break new legal ground that more risk averse class action attorneys may not have.

264. See *id.* at 224, 224 n.19; Jennifer Surane, *Visa, Mastercard Face Next Fight After \$6.2 Billion Settlement*, BLOOMBERG (Sept. 18, 2018), <https://www.bloomberg.com/news/articles/2018-09-18/visa-mastercard-reach-6-2-billion-settlement-over-swipe-fees>.

265. See, e.g., William E. Kovacic, Former Chairman, FTC, Panel Discussion at the Antitrust and 21st Century Bigness: Dealing with Tech Platforms in a Globalized World Conference (Feb. 28, 2020).

266. See *supra* Part VII.

Fourth, agencies should pay particular attention to evidence that helps small players. While information is generally hard to come by for class attorneys, big plaintiffs tend to be better off. The more sizable of the class plaintiffs—for example the few big app developers such as Epic Games, Spotify, and Netflix—have greater information and incentive due to their higher stake in the litigation.²⁶⁷ Indeed, Spotify's EU antitrust complaint and Epic's lawsuit have produced significant information about Apple's anticompetitive conduct that plaintiffs can use.²⁶⁸ In their investigations and litigations, the FTC and DOJ should thus spend significant amounts of time on possible LRAs and relevant facts that smaller players such as individual developers and consumers may not have the resources and capabilities to develop on their own. This focus can better make up for the gaps in private class action incentives and improve the efficiency of the division of labor between public and private antitrust enforcement in today's consumer platform economy.

IX. CONCLUSION

Before the age of the smartphone, two gigantic platforms successively dominated the tech world: IBM and Microsoft. IBM was the giant of mainframe computers that commanded the market. As the DOJ was strongly considering an antitrust lawsuit against the company for illegal tying, IBM preemptively unbundled its hardware and software offerings and opened up its software platform to outsiders. That move created the conditions for Microsoft's operating system software to flourish.²⁶⁹ In the late 1990s, similarly motivated by what many believe was the threat of antitrust lawsuit and the desire to appease regulators, Microsoft opened up and made its Office software suite available not only on Windows but also on Apple's computer operating system.²⁷⁰ This helped Apple survive its near-bankruptcy and made it possible for the company to create the iPhone a decade later.

In both cases, the dominant platform, facing imminent antitrust enforcement, opened itself to potential competitors. Both moves led to the creation of the next great platform. Antitrust law was doing its work even before litigation happened—although lawsuits were ultimately brought in both cases, a refreshing reminder that anticompetitive conduct will eventually be

267. See Coffee, *supra* note 244, at 223.

268. See *Spotify Timeline*, *supra* note 132; Hollister, *supra* note 106.

269. See Ben Thompson, *Facebook's FTC Fine, Apple and Microsoft's Mistake, IBM's Unbundling*, STRATECHERY (July 16, 2019), <https://stratechery.com/2019/facebooks-ftc-fine-apple-and-microsofts-mistake-ibms-unbundling>.

270. See *id.*

punished. This is how competition and innovation happen when antitrust law works.

But U.S. antitrust law has not worked in a long time. Antitrust enforcement has fallen to its slowest rate since 1970s.²⁷¹ The Bush administration brought “a grand total of zero anti-monopoly antitrust cases” over eight years, and antitrust enforcement has not recovered ever since.²⁷² Without the threat of antitrust law, tech platforms have been happily collecting their monopoly rents without fear of punishment.

Recent investigations are changing that, and a new toolbox is needed. This Note outlined the various harms tech platforms such as Apple have brought to consumers and competition. It also aimed to transform outdated antitrust assumptions with findings from the modern consumer platform economy. With a renewed understanding of competition dynamics, courts and enforcement agencies would be better equipped to address the challenges of the twenty-first century.

The free market does not always work on its own. With big data, armies of Ph.D. economists, and sharp understandings of consumer vulnerabilities, tech giants know the rules and loopholes of the market inside out. To build a fair marketplace where competition delivers innovation and consumer welfare, antitrust law must set the right boundaries.

271. Kadhim Shubber, *US Antitrust Enforcement Falls to Slowest Rate Since 1970s*, FIN. TIMES (Nov. 28, 2018), <https://www.ft.com/content/27a0a34e-f2a0-11e8-9623-d7f9881e729f>.

272. Tim Wu, *THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE* 108–10 (2018).

WHY 72 INTELLECTUAL PROPERTY SCHOLARS SUPPORTED GOOGLE'S COPYRIGHTABILITY ANALYSIS IN THE *ORACLE* CASE

Pamela Samuelson[†] & Catherine Crump^{††}

ABSTRACT

In January 2020, 72 intellectual property scholars signed on to an *amicus curiae* brief in support of Google's position that it did not infringe Oracle's copyright when it incorporated parts of the Java Application Program Interface (API) into its Android software, an issue that came before the U.S. Supreme Court in *Google LLC v. Oracle America, Inc.*

In ruling that the declarations of the Java API at issue in this case, as well as the structure, sequence, and organization (SSO) embodied in the declarations, were protectable expression as a matter of U.S. copyright law, the Federal Circuit's 2014 *Oracle* decision adopted an erroneously narrow view of the Supreme Court's decision in *Baker v. Selden* and of congressional codification of *Baker's* exclusion of systems and methods from copyright's scope in 17 U.S.C. § 102(b). Precedents from the Ninth and Second Circuits have persuasively held that program interfaces necessary for program compatibility are unprotectable by copyright law, decisions that the Federal Circuit either misconstrued or ignored.

The Federal Circuit also had a mistaken understanding of the merger doctrine as applied in computer program copyright cases. Its view is irreconcilable with *Baker* and other persuasive decisions. Case law from numerous circuits recognizes that when the design choices of subsequent programmers are constrained by the interface designs embodied in earlier programs, the merger doctrine applies so that programmers can reuse elements necessary to achieve compatibility.

Because of the Federal Circuit's numerous errors in analyzing Google's copyrightability defense, this Article, like the brief from which it is drawn, concludes that the Supreme Court would have been justified in overturning the Federal Circuit's ruling on copyrightability grounds. (The Supreme Court instead decided the case for Google on the fair use issue.) Allowing programmers to reuse interfaces that enable compatibility promotes the ongoing

DOI: <https://doi.org/10.15779/Z38R49G952>

© 2021 Pamela Samuelson & Catherine Crump. The views expressed in this Article are original to the co-authors. Seventy-one other IP scholars, however, joined the brief, so our views of the issues were shared by others.

† Pamela Samuelson is Richard M. Sherman Distinguished Professor of Law, Berkeley Law. This Article is a derivative work of the Brief of 72 Intellectual Property Scholars as *Amici Curiae* in Support of Petitioner, *Google LLC v. Oracle America, Inc.*, No. 18-956 (U.S. Jan. 13, 2020). The names of the signatories are not included in this Article but can be found in the brief, available at <https://ssrn.com/abstract=3518887>. Although one of us (Samuelson) has written several articles on the *Oracle v. Google* case and other software copyright rulings, we decided that this much more concise analysis of the issues warranted publication as a standalone article. We thank our signatories for their support and very helpful editorial suggestions.

†† Catherine Crump is Clinical Professor of Law, Berkeley Law, and Director of the Samuelson Law, Technology & Public Policy Clinic.

progress in the field of computer programming as well as advancing the science of computing, in keeping with the constitutional purpose of copyright law.

TABLE OF CONTENTS

| | | |
|-------------|--|------------|
| I. | INTRODUCTION | 415 |
| II. | U.S. SUPREME COURT PRECEDENTS, THE TEXT OF THE COPYRIGHT ACT, AND SOUND COPYRIGHT POLICY REQUIRE THE EXCLUSION OF PROGRAM INTERFACES FROM COPYRIGHT'S SCOPE | 417 |
| A. | THE SUPREME COURT ORIGINATED THE EXCLUSION OF SYSTEMS, METHODS, AND THEIR CONSTITUENT ELEMENTS FROM THE SCOPE OF COPYRIGHT PROTECTION..... | 419 |
| B. | CONGRESS CODIFIED THE WELL-ESTABLISHED EXCLUSION OF SYSTEMS AND METHODS IN § 102(b) | 421 |
| C. | THE FEDERAL CIRCUIT'S <i>ORACLE</i> DECISION IGNORED THE § 102(b) SYSTEM/METHOD EXCLUSIONS..... | 422 |
| | 1. <i>The Method and System Exclusions of § 102(b) Avert Patent/ Copyright Overlaps.....</i> | 424 |
| | 2. <i>Unprotectable Elements in Computer Programs Must Be Filtered Out Before Assessing Infringement.....</i> | 424 |
| | 3. <i>Methods and Systems Are Part of Program Structure, Sequence, and Organization, So SSO Obscures Rather Than Clarifies Expressive Aspects of Software</i> | 425 |
| D. | KEY POST-1976 ACT DECISIONS FOLLOW <i>BAKER</i> IN EXCLUDING METHODS, SYSTEMS, AND THEIR CONSTITUENT ELEMENTS FROM COPYRIGHT'S SCOPE..... | 425 |
| E. | CONSISTENT WITH <i>BAKER</i> AND § 102(b), PROGRAM INTERFACES SHOULD BE CONSIDERED UNPROTECTABLE PROCEDURES, METHODS, OR SYSTEMS..... | 428 |
| III. | THE FEDERAL CIRCUIT'S MERGER ANALYSIS IS IRRECONCILABLE WITH <i>BAKER</i> AND OTHER PERSUASIVE DECISIONS..... | 429 |
| A. | THE FEDERAL CIRCUIT'S ANALYSIS OF THE MERGER DOCTRINE IS AT ODDS WITH <i>BAKER</i> IN THREE KEY RESPECTS..... | 430 |
| B. | THE MERGER DOCTRINE PROVIDES A SOUND BASIS FOR HOLDING THAT PROGRAM INTERFACES THAT ENABLE COMPATIBILITY ARE UNCOPYRIGHTABLE | 432 |
| C. | THE FEDERAL CIRCUIT IGNORED THE DISTRICT COURT'S FACT FINDINGS THAT SUPPORTED ITS HOLDING THAT THE | |

| | |
|---|------------|
| INTERFACES AT ISSUE WERE UNPROTECTABLE UNDER THE MERGER DOCTRINE..... | 435 |
| D. THE DISTRICT COURT PROPERLY HELD THAT NAMES AND SHORT PHRASES ARE NOT PROTECTABLE BY COPYRIGHT..... | 435 |
| IV. CONCLUSION..... | 437 |

I. INTRODUCTION

The Federal Circuit's ruling against Google's copyrightability defense in *Oracle America, Inc. v. Google Inc.*¹ misconstrued the text of the Copyright Act, Supreme Court rulings, as well as software copyright case law persuasively establishing that interfaces that enable compatibility among programs are unprotectable by copyright law, thereby disrupting settled expectations of this \$845 billion industry.² The U.S. Supreme Court granted Google's petition for certiorari and reviewed the Federal Circuit's decision in its October term 2020, ultimately deciding the case on fair use grounds.³

1. 750 F.3d 1339 (Fed. Cir. 2014). For a detailed discussion of this case and the Federal Circuit's ruling on copyrightability, see, for example, Pamela Samuelson, *Functionality and Expression in Computer Programs: Refining the Tests for Software Copyright Infringement*, 31 BERKELEY TECH. L.J. 1215 (2016). After the Federal Circuit's copyrightability ruling in 2014, Google petitioned the Supreme Court for review, which the Court denied in 2015. Subsequently, a jury found that Google's use of the Java API packages was a fair use, but the Federal Circuit reversed, concluding that Google's use was not fair as a matter of law. *Oracle Am., Inc. v. Google LLC*, 886 F.3d 1179, 1186 (Fed. Cir. 2018). The Supreme Court agreed to review the Federal Circuit's decisions regarding both copyrightability and fair use. *Id.*, cert. granted, 140 S. Ct. 520 (U.S. Nov. 15, 2019) (No. 18-956). This Article, like the brief from which it is drawn, focuses on the copyrightability issue only. While this Article was in process, the Court issued its opinion on April 5, 2021, reversing the Federal Circuit's fair use ruling and holding that Google's use of the Sun Java APIs was fair use as a matter of law. *Google LLC v. Oracle Am., Inc.*, 141 S. Ct. 1183 (2021), rev'g 886 F.3d 1179 (Fed. Cir. 2018). Although the majority opinion written by Justice Breyer stated that it assumed, "for argument's sake," that the Java APIs were copyrightable, 141 S. Ct. at 1190, its fair use analysis employed reasoning and language that appear to support § 102(b) and merger arguments. *Id.* at 1192–93, 1201–02. Further discussion of the Court's opinion are beyond the scope of this Article. We remain convinced that the Court would have been justified in deciding this case on the § 102(b) and/or merger issues, as we believe the Federal Circuit's analysis of these issues is so deeply flawed.

2. See BSA Foundation, *Software: Growing US Jobs and the GDP* (Sept. 2019), <https://software.org/wp-content/uploads/2019SoftwareJobs.pdf> (based on 2018 data).

3. Oral argument in the *Google* case was originally scheduled for March 24, 2020, but because of the coronavirus pandemic, the Court moved this matter to its calendar for the October term 2020. On May 4, 2020, the Court requested supplemental briefing on the appropriate standard of review of the jury's fair use finding in favor of Google. Both parties

Until the Court of Appeals for the Federal Circuit's 2014 *Oracle* decision, software developers felt free to compete and innovate in the development of compatible software because major decisions from the Courts of Appeals for the Second and Ninth Circuits had established that copyright law does not protect software interfaces that enable the development of compatible programs.⁴ These cases and their progeny recognized that unlike conventional literary works, computer programs are highly utilitarian.⁵ They embody many copyright-unprotectable elements, such as compatibility-enabling interfaces, that must be filtered out before making infringement determinations. Computer programs consequently receive a relatively "thin" scope of copyright protection to ensure that subsequent programmers can freely reuse unprotectable elements in developing their own programs. As a matter of copyright law, the pro-compatibility decisions are sound as they facilitate fair competition by those who write new code while preserving copyright's role in protecting software from piracy and other wrongful appropriations.

The Federal Circuit's 2014 *Oracle* decision was a radical departure from these precedents and directly contradicted their rulings. It adopted an unduly narrow view of the Supreme Court's ruling in *Baker v. Selden*,⁶ which excluded methods, systems, and their constituent elements from copyright's scope. It ignored Congress's codification of the method/system exclusions.⁷ It misconstrued the case law properly interpreting those exclusions in relation to program interfaces.⁸ The Federal Circuit also misapplied the merger doctrine and case law persuasively holding that interfaces that enable compatibility are unprotectable by copyright law. Because of the Federal Circuit's numerous

filed their respective supplemental letter briefs on August 7, 2020. The Court heard oral argument on October 7, 2020.

4. *See* *Comput. Assocs. Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693 (2d Cir. 1992); *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992).

5. *See* *Altai*, 982 F.2d at 712; *Accolade*, 977 F.2d at 1524.

6. 101 U.S. 99 (1880).

7. 17 U.S.C. § 102(b).

8. The District Court in *Oracle* relied on both the § 102(b) method/system exclusions and the merger doctrine in its analysis of the copyrightability issue. This practice is common. Once an author devises a particular method or system, there may be relatively few ways to express it. *See, e.g.*, *Ho v. Taflove*, 648 F.3d 489, 497–99 (7th Cir. 2011) (analyzing the copyrightability of a scientific model and equation under § 102(b) and the merger doctrine); *Hutchins v. Zoll Med. Corp.*, 492 F.3d 1377, 1383–85 (Fed. Cir. 2007) (analyzing the copyrightability of the process of CPR and standard instructions for performing that process under § 102(b) and the merger doctrine); *MiTek Holdings, Inc. v. Arce Eng'g Co., Inc.*, 89 F.3d 1548, 1556 n.19, 1557 n.20 (11th Cir. 1996) (analyzing application of copyright to a command tree structure under § 102(b) and the merger doctrine); *Atari Games Corp. v. Nintendo of Am., Inc.*, 975 F.2d 832, 839–40 (Fed. Cir. 1992) (analyzing the copyrightability of a data stream for unlocking a console under both § 102(b) and the merger doctrine).

errors in analyzing Google's copyrightability defense, the Supreme Court would have been justified in overturning the Federal Circuit's ruling. Programmers should have to write their own implementation code, as Google did, but interfaces that enable compatibility should be free from copyright restrictions.

II. U.S. SUPREME COURT PRECEDENTS, THE TEXT OF THE COPYRIGHT ACT, AND SOUND COPYRIGHT POLICY REQUIRE THE EXCLUSION OF PROGRAM INTERFACES FROM COPYRIGHT'S SCOPE

Freedom to compete and innovate in the development of compatible software was first recognized in the Second Circuit's landmark decision in *Computer Associates International, Inc. v. Altai, Inc.*⁹ It held that interfaces of computer programs that enable compatibility are unprotectable by copyright law.¹⁰ It concluded that Altai did not infringe by reimplementing the same interface as Computer Associates in its competing scheduling program.¹¹ Later that year, the Ninth Circuit in *Sega Enterprises, Ltd. v. Accolade, Inc.*,¹² which cited approvingly to *Altai*, decided that the functional requirements for achieving compatibility are unprotectable by copyright law.¹³ It characterized these requirements as "interface procedures" that are excluded from copyright protection under 17 U.S.C. § 102(b).¹⁴ Accolade was thus free to adapt its videogames so that they could run on Sega's popular platform. Other courts followed these precedents.¹⁵ *Altai* and *Accolade* recognized that the essentially utilitarian nature of computer programs means they embody many copyright-unprotectable elements, including interfaces that enable compatibility, hence programs enjoy "a relatively weak barrier against public access" to those unprotected elements.¹⁶ This ensures that subsequent programmers can reuse those elements in developing their own programs.

9. 982 F.2d 693 (2d Cir. 1992).

10. *Id.* at 710.

11. *Id.* at 715.

12. 977 F.2d 1510 (9th Cir. 1992).

13. *Id.* at 1522.

14. *Id.*

15. *See, e.g.,* Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1547 (11th Cir. 1996) (recognizing the need for compatibility between the defendant's application program and an operating system program).

16. *Altai*, 982 F.2d at 712; *see also* *Accolade*, 977 F.2d at 1527 (finding that the incorporation of utilitarian elements in a computer program did not merit copyright protection).

Relying on these precedents and the method/system exclusions of 17 U.S.C. § 102(b), Google believed that the declarations of the Java API used in its Android software and the structure, sequence, and organization (SSO) embodied in the declarations were not within the scope of protection that copyright law provides to the work of authorship at issue,¹⁷ namely, Java 2 SE (Java SE), whose contents include program code, specifications of the Java packages and their classes and methods, and related documentation.

The District Court made findings of fact from which it concluded that these declarations were not within the scope of protection that copyright law provided to Java SE.¹⁸ It regarded the declarations as constituent elements of an interface system or method that should be excluded from the scope of copyright protection under 17 U.S.C. § 102(b).¹⁹ This ruling is consistent with the Supreme Court's decision in *Baker v. Selden*, which held that the selection and arrangement of columns and headings in Selden's bookkeeping forms were not within the scope of protection that copyright law provided to his book.²⁰ The ruling is also consistent with congressional codification of *Baker's* exclusion of methods and systems and with the Ninth Circuit's characterization of program interfaces as unprotectable procedures under § 102(b) in *Accolade*.²¹ It is also consistent with the views of an information technology industry association known as the American Committee for Interoperable Systems (ACIS), whose founding member, Sun Microsystems, created the Java API.²² In an amicus brief, ACIS advised the Court that "it can accurately be said that the interface specification is the 'system' or 'method of operation' that is 'expressed' by the program code."²³

17. According to the District Court, "all agree[] that Google had not literally copied the software but had instead come up with its own implementations of the 37 API packages." *Oracle Am., Inc. v. Google Inc.*, 872 F. Supp. 2d 974, 975 (N.D. Cal. 2012). This is consistent with computer scientists' conception of the declarations as interfaces. *See* Brief of 78 Amici Curiae Computer Scientists in Support of Petitioner at 6, *Google LLC v. Oracle Am., Inc.*, No. 18-956 (U.S. Feb. 25, 2019) [hereinafter 78 Computer Scientists Cert. Brief].

18. *Oracle*, 872 F. Supp. 2d at 976.

19. *Id.*

20. 101 U.S. 99, 106 (1880).

21. *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1522 (9th Cir. 1992).

22. Brief Amici Curiae of American Committee for Interoperable Systems and Computer & Communications Association in Support of Respondent at 1, n.1, *Lotus Dev. Corp. v. Borland Int'l, Inc.*, 516 U.S. 233 (1996) (No. 94-2003) (listing ACIS membership).

23. *Id.* at 19.

A. THE SUPREME COURT ORIGINATED THE EXCLUSION OF SYSTEMS, METHODS, AND THEIR CONSTITUENT ELEMENTS FROM THE SCOPE OF COPYRIGHT PROTECTION

Perris v. Hexamer was the first Supreme Court decision to rule that copyright protection does not extend to a system and its constituent parts embodied in a copyrighted work.²⁴ Perris sued Hexamer for using the same symbol system in a map of Philadelphia as Perris had used in a map of certain wards of New York City.²⁵ Both maps depicted the layout of lots and buildings using a set of symbols and color-coding to identify different types of buildings to aid in risk assessment for fire insurance purposes.²⁶ The Court concluded that Perris had “no more an exclusive right to use the form of the characters they employ to express their ideas upon the face of the map, than they have to use the form of type they select to print the key.”²⁷ After all, Hexamer had not copied Perris’s map but only “use[d] to some extent their system of arbitrary signs and their key.”²⁸ The Court considered this system to be a “useful contrivance[] for the despatch of business.”²⁹ It did not matter how original that system might have been or how many other symbol systems could have been devised. That system was simply not protectable by copyright law.

Soon thereafter, the Court reviewed a similar infringement claim in *Baker*. Because *Baker* is such a foundational case and its proper interpretation is disputed by the litigants, we provide some details about the case. Prior to Charles Selden’s claimed invention of a novel bookkeeping system, the standard process by which officials kept account books was slow and inefficient. Bookkeepers had to record information about each transaction in a journal for accounts of that kind and then record details again in a ledger where all transactions were recorded in sequential fashion.³⁰ Because the relevant information was spread out over multiple volumes, it was difficult to prepare a balance sheet for each period and to detect errors or fraud.

Selden’s key innovation was figuring out a way (as the book’s title, *Selden’s Condensed Ledger, or Bookkeeping Simplified*, suggests) to condense the journals

24. 99 U.S. 674 (1879).

25. *Id.* at 675.

26. *Id.*

27. *Id.* at 676.

28. *Id.*

29. *Id.* at 675.

30. Supreme Court Record at 92, 106, *Baker v. Selden*, 101 U.S. 99 (1880) [hereinafter Record]. For further details about the *Baker* litigation, see Pamela Samuelson, *The Story of Baker v. Selden: Sharpening the Distinction Between Authorship and Invention*, in INTELLECTUAL PROPERTY STORIES 159 (Rochelle Cooper Dreyfuss & Jane C. Ginsburg eds., 2005) [hereinafter *Baker Story*]. To view simulations of the relevant forms, see *id.* at 170–71.

and ledger, so that users could record pertinent information about transactions and accounts on one page or two adjoining pages.³¹ It enabled a much more efficient accounting process, making the preparation of trial balances and detection of errors and fraud much easier.³²

Selden's sense of the magnitude of his achievement was expressed in the preface to his book: "To greatly simplify the accounts of extensive establishments doing credit business . . . would be a masterly achievement, worthy to be classed among the greatest benefactions of the age."³³ The preface revealed that Selden had sought a patent on forms embodying his system to "prevent their indiscriminate use by the public."³⁴

Although Selden knew about Baker's competing book and similar forms during his lifetime, it was his widow who charged Baker with infringement, claiming that "the ruled lines and headings, given to illustrate the system, are a part of the book, and, as such, are secured by the copyright; and that no one can make or use similar ruled lines and headings . . . without violating the copyright."³⁵

The Court had no doubt that a work on bookkeeping could be copyrighted or that it would be "a very valuable acquisition to the practical knowledge of the community."³⁶ But the Court perceived "a clear distinction between the book, as such, and the [useful] art which it is intended to illustrate."³⁷ Copyright law could protect the author's explanation of a useful art, but not the useful art itself, no matter how creative it was. "To give to the author of the book an exclusive property in the [useful] art described therein," the Court said, "would be a surprise and a fraud upon the public. That is the province of letters-patent, not of copyright."³⁸ That Mrs. Selden intended to assert patent-like rights through copyright is evident from her announcement to Baker's customers that they too were infringers.³⁹ Had Selden obtained the patent he sought, it would have given him and his heirs exclusive rights to control uses of the system, as well as making and selling the forms that embodied the system.⁴⁰ But no such patent had been issued.

31. *Id.* at 160.

32. *Id.*

33. Record, *supra* note 30, at 21.

34. *Id.* at 21–22.

35. *Baker v. Selden*, 101 U.S. 99, 101 (1880).

36. *Id.* at 102.

37. *Id.*

38. *Id.*

39. Record, *supra* note 30, at 79–80.

40. *See Baker Story*, *supra* note 30, at 174.

The Court recognized that Selden's claim seemed plausible because of the "peculiar nature of the [useful] art described in [his] books" in which "the illustrations and diagrams employed happen to correspond more closely than usual with the actual work performed by the operator who uses the art."⁴¹ Someone who kept books using Selden's method would necessarily use forms with the same or substantially similar headings and columns. Usually, the Court observed, useful arts are "represented in concrete forms of wood, metal, stone, or some other physical embodiment."⁴² But "the principle is the same in all" regardless of whether the useful art is embodied in a writing or in metal.⁴³ The Court concluded that Selden's system was unprotectable by copyright law, as were the ruled lines and headings that instantiated the system.⁴⁴

Baker illustrates why copyright law should allow second comers to build upon methods and systems embodied in a first author's works and why authors of writings on methods and systems should not have too much control over subsequent adaptations of these creations. Selden's forms may have been a substantial improvement over the old-fashioned bookkeeping methods previously in use, but they were only one stage in the evolving art of bookkeeping. Selden's death meant that any further innovation in this field would have to come from others. Baker advanced the state of the art by redesigning the forms so that entries could be made as transactions occurred rather than having to wait until the end of the week or month as Selden's forms required.⁴⁵ Baker went on to write other books and he, not Selden, can be credited with having advanced the state of the art of bookkeeping in the nineteenth century.⁴⁶ Had Mrs. Selden prevailed, further improvements in the bookkeeping field might well have been stunted until Selden's copyrights expired. This outcome would have disserved both patent and copyright goals, as it would have slowed progress in the science and useful art of bookkeeping.

B. CONGRESS CODIFIED THE WELL-ESTABLISHED EXCLUSION OF SYSTEMS AND METHODS IN § 102(b)

Dozens of cases followed *Baker's* conclusion that methods, systems, and their constituent elements are beyond the scope of copyright protection in writings that embody useful arts. Two courts, for example, rejected claims of infringement against authors who wrote books about the plaintiffs' original

41. *Baker*, 101 U.S. at 104.

42. *Id.* at 105.

43. *Id.*

44. *Id.* at 106.

45. *Baker Story*, *supra* note 30, at 162.

46. *See id.* at 169, 193 n.76.

shorthand systems: *Brief English Systems, Inc. v. Owen* and *Griggs v. Perrin*.⁴⁷ Another court, in *Aldrich v. Remington Rand, Inc.*, dismissed a claim of infringement for copying the plaintiff's tax record system, which Aldrich claimed to be "the most modern and efficient system of property revaluation for tax purposes."⁴⁸ Numerous other *Baker*-inspired cases ruled that original methods and systems for contests, games, rules, and strategies for playing games were beyond the scope of copyright protection.⁴⁹

The *Baker*-inspired exclusions of methods and systems from copyright's scope was so well-established that Congress decided to codify these exclusions in the Copyright Act of 1976. Thus, 17 U.S.C. § 102(b) provides: "In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work." By codifying the method and system exclusions in § 102(b), Congress sought to ensure that the copyright in computer software and other works that embody functional elements would not be construed too broadly.⁵⁰ Courts in software copyright cases accordingly are charged with applying the § 102(b) exclusions as meaningful limits on the scope of copyright protection available to computer programs.

C. THE FEDERAL CIRCUIT'S *ORACLE* DECISION IGNORED THE § 102(b) SYSTEM/METHOD EXCLUSIONS

In *Oracle*, the Federal Circuit ruled that the Java declarations used by Google were copyright-protectable expression as a matter of law.⁵¹ In so doing, the court articulated a very narrow understanding of § 102(b) and misconstrued the way in which the District Court analyzed the copyrightability issue in this case.

The Federal Circuit's *Oracle* opinion focused on whether copyright extends at all to works that incorporate functional elements.⁵² We certainly agree with the Federal Circuit that § 102(b) should not be interpreted so literally that it

47. See *Brief English Sys., Inc. v. Owen*, 48 F.2d 555 (2d Cir. 1931); *Griggs v. Perrin*, 49 F. 15 (C.C.N.D.N.Y. 1892).

48. 52 F. Supp. 732, 733 (N.D. Tex. 1942).

49. See Pamela Samuelson, *Why Copyright Law Excludes Systems and Processes from the Scope of Its Protection*, 85 TEX. L. REV. 1921, 1936–44 (2007) (reviewing post-*Baker* method/system copyright cases).

50. See H.R. REP. NO. 94-1476, at 57 (1976); S. REP. NO. 94-473, at 54 (1976).

51. *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1368 (Fed. Cir. 2014).

52. *Id.* at 1367. The Federal Circuit seemed to characterize the District Court's order as suggesting that computer programs are per se uncopyrightable due to their functional aspects, *id.*, but that overbroad characterization misconstrues the District Court's analysis, see Samuelson, *supra* note 1, at 1256.

would deprive authors of machine-executable programs of the copyrights that Congress intended them to have just because programs are machine processes.⁵³

The Federal Circuit's *Oracle* decision may have properly quoted the text of § 102(b),⁵⁴ but it treated ideas as the only unprotectable element of copyrighted software, giving no substantive meaning to the other seven terms of exclusion.⁵⁵ This is, as Justice Scalia once stated, “a stark violation of the elementary principle that requires an interpreter ‘to give effect, if possible, to every clause and word of a statute,’” to which he added:

Lawmakers sometimes repeat themselves . . . [They] do not, however, tend to use terms that “have no operation at all.” So while the rule against treating a term as a redundancy is far from categorical, the rule against treating it as a nullity is as close to absolute as interpretive principles get.⁵⁶

When a statute such as § 102(b) specifically identifies several categories of uncopyrightable elements and says “[i]n no case” should any of these be within the scope of copyright’s protection, reading all but one of the terms out of the statute, as the Federal Circuit did in *Oracle*, violates this rule. It thus failed to be “deferential to the judgment of Congress in the realm of copyright.”⁵⁷

Although the text of § 102(b) is unambiguous in light of the holdings in *Baker* and its progeny, it is worth noting that Congress added the method/system exclusions to the statute, in part, to allay concerns about the risk of an excessive scope of copyright protection for software:

Some concern has been expressed lest copyright in computer programs should extend protection to the methodology or processes adopted by the programmer, rather than merely to the “writing” expressing his ideas. Section 102(b) is intended, among other things, to make clear that the expression adopted by the programmer is the copyrightable element in a computer program, and that the actual processes or methods embodied in the program are not within the scope of the copyright law.⁵⁸

53. See *Oracle*, 750 F.3d at 1367.

54. *Id.* at 1354.

55. *Id.* at 1367.

56. *King v. Burwell*, 576 U.S. 473, 502 (2015) (Scalia, J., dissenting) (citations omitted).

57. *Eldred v. Ashcroft*, 537 U.S. 186, 198 (2003).

58. H.R. REP. NO. 94-1476 at 57 (1976); S. REP. NO. 94-473 at 54 (1975). During hearings on copyright revision bills, several witnesses recommended adoption of a specific provision to limit the scope of copyright protection in computer programs. See *Copyright Law Revision, Hearings before the Subcomm. on Patents, Trademarks, & Copyrights of the S. Comm. on the Judiciary*, 90th Cong. 196–97 (1967) (statement of Arthur R. Miller). Miller foresaw a risk that

The Federal Circuit tellingly recited only that part of the legislative history stating that § 102(b) codified the idea/expression distinction⁵⁹ and omitted congressional expressions of concern about excessive copyright protection for software. It overlooked the Supreme Court's directive not to "alter the delicate balance Congress has labored to achieve."⁶⁰

1. *The Method and System Exclusions of § 102(b) Avert Patent/Copyright Overlaps*

Consistent with the *Baker* tradition, codification of the system/method exclusions in § 102(b) aims, in part, to ensure that domains of copyright and patent protection for programs should be kept separate. The Federal Circuit once recognized this purpose in *Atari Games Corp. v. Nintendo of America, Inc.*⁶¹ After quoting § 102(b)'s exclusion of procedures, processes, systems, and methods of operation, it stated that patent and copyright laws protect "distinct aspects" of programs.⁶² The role of copyright, said the court, was to protect program expression, not any methods or processes that might be eligible for patenting under the Patent Act.⁶³

The Federal Circuit's *Oracle* decision, however, instead seemingly endorsed the view that computer program innovations such as interfaces were eligible for both copyright and patent protection.⁶⁴ This was pertinent because both Sun and Oracle had obtained utility patents on program interfaces.⁶⁵

2. *Unprotectable Elements in Computer Programs Must Be Filtered Out Before Assessing Infringement*

The Federal Circuit's *Oracle* decision also failed to recognize that the utilitarian nature of computer programs differentiates them from conventional literary works because programs contain many functional design elements, including methods and systems, that are beyond the scope of copyright under

courts would interpret copyright to extend to computer processes "that the program uses to achieve a functional goal," which would confer "patentlike [sic] protection under the guise of copyright." *Id.* at 197. He recommended that Congress should affirm that copyright would extend "solely to duplication or replication of the program" and not to "the art, process or scheme that is fixed in the program" because only patent law could protect "systems, schemes, and processes." *Id.* at 197, 199. For a fuller discussion of the genesis of § 102(b) exclusions, see Samuelson, *supra* note 49, at 1944–61.

59. *Oracle*, 750 F.3d at 1357.

60. *Stewart v. Abend*, 495 U.S. 207, 230 (1990).

61. 975 F.2d 832 (Fed. Cir. 1992).

62. *Id.* at 839.

63. *Id.*

64. *Oracle*, 750 F.3d at 1380 (erroneously quoting *Mazer v. Stein*, 347 U.S. 201, 217 (1954), which considered only potential design patent and copyright overlaps).

65. *Oracle Am., Inc. v. Google Inc.*, 872 F. Supp. 2d 974, 996 (N.D. Cal. 2012).

§ 102(b) and other doctrines.⁶⁶ The higher quantum of unprotectable elements in programs, as compared with novels, explains why courts such as the Second Circuit in *Altai* have directed that numerous types of unprotectable elements of programs be “filtered out” before deciding infringement claims in software copyright cases.⁶⁷ Although the Federal Circuit criticized the lower court for not following *Altai*,⁶⁸ the appellate court itself performed no filtration whatsoever.

3. *Methods and Systems Are Part of Program Structure, Sequence, and Organization, So SSO Obscures Rather Than Clarifies Expressive Aspects of Software*

The Federal Circuit accepted without question Oracle’s claim that the SSO of computer programs is protectable expression.⁶⁹ By contrast, the Second Circuit wisely recognized in *Altai* that SSO is not a useful term with which to distinguish nonliteral elements of programs that may be expressive enough to be copyright-protectable from nonliteral elements that are excluded from copyright protection.⁷⁰

By their very nature, methods and systems, when embodied in computer programs, are parts of SSO. Under the Federal Circuit’s *Oracle* decision, it would be trivially easy for software developers to claim SSO copyright protection in methods or processes for which they failed to seek patent protection, or even to claim SSO copyright protection in processes for which patent protection is now unavailable in the aftermath of *Alice Corp. v. CLS Bank International*.⁷¹ The Federal Circuit’s ruling thus undermines the Supreme Court’s holding in *Alice*.

D. KEY POST-1976 ACT DECISIONS FOLLOW *BAKER* IN EXCLUDING METHODS, SYSTEMS, AND THEIR CONSTITUENT ELEMENTS FROM COPYRIGHT’S SCOPE

An exemplary decision applying *Baker* and § 102(b) to exclude systems and their constituent parts from the scope of copyright is *Bikram’s Yoga College of India, L.P. v. Evolution Yoga, LLC*.⁷² Similar to *Baker*, in which Selden claimed copyright in the selection and arrangement of headings and columns in his

66. See, e.g., *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1524 (9th Cir. 1992).

67. *Comput. Assocs. Int’l, Inc. v. Altai, Inc.*, 982 F.2d 693, 706–11(2d Cir. 1992).

68. *Oracle*, 750 F.3d at 1358.

69. *Id.* at 1365.

70. *Altai*, 982 F.2d at 706.

71. 573 U.S. 208, 212 (2014) (holding a computer program patent-ineligible because its claim merely consisted of an abstract idea implemented on a generic computer).

72. 803 F.3d 1032 (9th Cir. 2015).

novel bookkeeping forms, Bikram Choudhury claimed copyright in a sequence of twenty-six yoga poses and two breathing exercises described and illustrated in books and videos.⁷³ After Evolution Yoga began teaching the same sequence, Bikram's Yoga College sued it for infringement. Relying on *Baker* and its codification in § 102(b), the Ninth Circuit held that the Bikram Yoga Sequence was “not a proper subject of copyright protection.”⁷⁴

It did not matter whether Choudhury's arrangement of poses and breathing exercises was beautiful or graceful.⁷⁵ Nor did it matter that “the Sequence may possess many constituent parts,” for “[v]irtually any process or system could be dissected in a similar fashion.”⁷⁶ Also irrelevant was “that similar results could be achieved through a different organization of yoga poses and breathing exercises.”⁷⁷ What mattered was that “[a]n essential element of this ‘system’ is the order in which the yoga poses and breathing exercises are arranged.”⁷⁸ Choudhury's books directed his pupils to perform the yoga moves “in the strict order given in this book.”⁷⁹ Choudhury had, moreover, repeatedly characterized his sequence as a method or system for improving health and well-being, which rendered the system and its constituent parts too functional for copyright protection.⁸⁰

As in *Baker*, the Ninth Circuit in *Bikram* opined that to get exclusive rights in a functional system, such as the Yoga Sequence, it would be necessary to obtain a patent.⁸¹ As in *Baker*, copyright protected Choudhury's explanation of his method or system, not the system itself or downstream uses of it. His books invited readers to practice the method the books taught.⁸² Echoing *Baker*, the Ninth Circuit said that this objective “would be frustrated if the knowledge could not be used without incurring the guilt of piracy of the book.”⁸³ “Consumers would have little reason to buy Choudhury's book if Choudhury held a monopoly on the practice of the very activity he sought to popularize,”⁸⁴ just as it would make little sense for consumers to buy Selden's book unless

73. *Id.* at 1035–36.

74. *Id.* at 1034. *Bikram* discusses *Baker* and its progeny. *Id.* at 1037–38.

75. *Id.* at 1040.

76. *Id.* at 1041.

77. *Id.* at 1042.

78. *Id.* at 1039.

79. *Id.*

80. *Id.* at 1038–39.

81. *Id.* at 1039–40.

82. *Id.* at 1035.

83. *Id.* at 1041 (quoting *Baker v. Selden*, 101 U.S. 99, 103 (1880)).

84. *Id.*; see also *Ho v. Taflove*, 648 F.3d 489, 498–99 (7th Cir. 2011) (holding a scientific model and its constituent elements unprotectable by copyright law); *Palmer v. Braun*, 287 F.3d 1325, 1334 (11th Cir. 2002) (holding meditation exercises were uncopyrightable processes).

they would thereby have the right to make use of the system and the forms that embodied it.

Consistent with *Bikram* was the Ninth Circuit's *Accolade* decision, which stated that program "interface procedures" that constituted "the functional requirements for [achieving] compatibility" were unprotectable by copyright law under 17 U.S.C. § 102(b).⁸⁵ While these statements appeared in a ruling that *Accolade*'s reverse engineering of Sega program code was fair use, they were not mere dicta nor of only slight importance to the outcome of the fair use ruling, as the Federal Circuit asserted.⁸⁶ The statements were the very linchpin of the *Accolade* ruling. *Accolade*'s disassembly and reverse engineering of Sega object code was legitimate because disassembly was "necessary in order to understand the functional requirements for Genesis compatibility."⁸⁷

The Ninth Circuit explained that "[i]f disassembly of copyrighted object code is *per se* an unfair use, the owner of the copyright gains a *de facto* monopoly over the functional aspects of his work—aspects that were expressly denied copyright protection by Congress."⁸⁸ Channeling *Baker*, the Ninth Circuit said that if Sega wanted to enjoy a legal monopoly over the interface procedures, it would have to "satisfy the more stringent standards imposed by the patent laws."⁸⁹ Allowing reverse engineering would enable new entrants such as *Accolade* to make compatible products available in the market.⁹⁰

Compatibility considerations were also important in *Lotus Development Corp. v. Borland International, Inc.*⁹¹ *Lotus* charged *Borland* with infringement for reusing the *Lotus* 1-2-3 menu command hierarchy for the emulation mode of its competing spreadsheet program.⁹² The District Court held that this hierarchy was protectable SSO because there were other ways to organize commands for spreadsheet program functions.⁹³

The First Circuit recognized that "*Borland* had to copy the *Lotus* menu command hierarchy" if it wanted to enable users "to operate its programs in

85. *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1522 (9th Cir. 1992).

86. *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1369 (Fed. Cir. 2014).

87. *Accolade*, 977 F.2d at 1526. *Baker* made account books based on a similar system to *Selden*'s in order to create a comparable and competitive product. *See Baker*, 101 U.S. at 101.

88. *Accolade*, 977 F.2d at 1526 (citing § 102(b)).

89. *Id.*

90. *See id.* at 1523–24; *see also Sony Comput. Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 605, 608 (9th Cir. 2000) (finding reverse engineering to achieve partial compatibility fair use); *Oracle Am., Inc. v. Google Inc.*, 872 F. Supp. 2d 974, 1000 (N.D. Cal. 2012) ("Contrary to Oracle, 'full compatibility' is not relevant to the Section 102(b) analysis.?).

91. 49 F.3d 807 (1st Cir. 1995), *aff'd by an equally divided Court*, 516 U.S. 233 (1996) (*per curiam*).

92. *Id.* at 810.

93. *Id.* at 810–11.

substantially the same way” as Lotus 1-2-3.⁹⁴ Borland’s emulation mode enabled users of the Lotus program who had constructed macros for common sequences of functions to port those macros to Borland’s program.⁹⁵ For those macros to be executable, Borland had to employ the same command terms arranged in exactly the same order. As the First Circuit explained:

Under the district court’s holding, if the user wrote a macro to shorten the time needed to perform a certain operation in Lotus 1-2-3, the user would be unable to use that macro . . . Rather, the user would have to rewrite his or her macro using that other program’s menu command hierarchy. This is despite the fact that the macro is clearly the user’s own work product.⁹⁶

The First Circuit concluded that this menu command hierarchy was an unprotectable method of operating a spreadsheet program under § 102(b).⁹⁷

Judge Boudin, concurring, observed:

If Lotus is granted a monopoly on this pattern, users who have learned the command structure of Lotus 1-2-3 or devised their own macros are locked into Lotus, just as a typist who has learned the QWERTY keyboard would be the captive of anyone who had a monopoly on the production of such a keyboard.⁹⁸

Lotus’ command hierarchy “look[s] hauntingly like the familiar stuff of copyright; but the ‘substance’ probably has more to do with problems presented in patent law.”⁹⁹

E. CONSISTENT WITH *BAKER* AND § 102(b), PROGRAM INTERFACES SHOULD BE CONSIDERED UNPROTECTABLE PROCEDURES, METHODS, OR SYSTEMS

The Supreme Court articulated a clean distinction in *Baker* between the copyrightable expression in Selden’s book and the uncopyrightable bookkeeping system, constituent elements of which were embodied in the forms.¹⁰⁰ A clean distinction is also possible in *Oracle*. Google and Java programmers around the world should be free to use the Java SE declarations

94. *Id.* at 816. The First Circuit invoked *Baker*, noting that “Lotus wrote its menu command hierarchy so that people could learn it and use it,” thus “fall[ing] squarely within the prohibition on copyright protection established in *Baker v. Selden* and codified by Congress in § 102(b).” *Id.* at 817.

95. *Id.* at 811–12.

96. *Id.* at 818.

97. *Id.* at 817–18.

98. *Id.* at 821 (Boudin, J., concurring).

99. *Id.* at 820.

100. *See Baker v. Selden*, 101 U.S. 99, 100–01 (1880).

to develop compatible programs, subject only to the norm that they must instantiate those interfaces in independently written code that copyright law protects from misappropriation.

Characterizing program interfaces as unprotectable procedures under § 102(b) is consistent with *Baker*, the text of § 102(b), and the case law properly interpreting it. The District Court's characterization of the declarations as methods or systems is similarly consistent, as was the ACIS amicus brief in *Borland*.¹⁰¹ Interfaces are methods insofar as they enable one program to function effectively with other software or with hardware. Some program interfaces are relatively simple, as in *Accolade*, while others are more complex, as in *Oracle*. But as the Supreme Court so aptly said in *Baker*, "the principle is the same in all."¹⁰² Allowing programmers to reuse interfaces that enable compatibility promotes the ongoing progress in the field of computer programming as well as advancing the science of computing, in keeping with the constitutional purpose of copyright law.¹⁰³

III. THE FEDERAL CIRCUIT'S MERGER ANALYSIS IS IRRECONCILABLE WITH *BAKER* AND OTHER PERSUASIVE DECISIONS

The merger doctrine is often traced to the Supreme Court's *Baker* decision.¹⁰⁴ In *Baker*, the Court concluded that the forms embodying Selden's bookkeeping system were unprotected by copyright law because using these or similar arrangements of columns and headings was necessary to implement the underlying system.¹⁰⁵ As the Court explained:

[W]here the [useful] art [a work] teaches cannot be used without employing the methods and diagrams used to illustrate the book, or such as are similar to them, such methods and diagrams are to be considered as *necessary incidents* to the art, and given therewith to the public; not given for the purpose of

101. See Brief Amici Curiae of American Committee for Interoperable Systems and Computer & Communications Association in Support of Respondent, *supra* note 22.

102. *Baker*, 101 U.S. at 105.

103. U.S. CONST. art. I, § 8, cl. 8.

104. See, e.g., *Arica Inst., Inc. v. Palmer*, 970 F.2d 1067, 1076 (2d Cir. 1992); Pamela Samuelson, *Reconceptualizing Copyright's Merger Doctrine*, 63 J. COPYRIGHT SOC'Y U.S.A. 417, 419–20 (2016). While *Baker* did not originate the term "merger," it nonetheless articulated principles congruent with what came to be known as the merger doctrine and that guide the outcome here.

105. *Baker*, 101 U.S. at 103.

publication in other works explanatory of the art, but for the purpose of practical application.¹⁰⁶

This “necessary incidents” language serves to prevent copyright from extending to unprotectable systems when the reuse of some expression is inseparable from the systems.

The Federal Circuit’s analysis of the merger doctrine in *Oracle* cannot be reconciled with *Baker*. It is, moreover, contrary to persuasive authorities recognizing the merger doctrine as a shield against infringement for software interfaces that enable the development of compatible programs. Consistent with these authorities, the District Court found that the declarations had to be identical for the functionality they enable to be available in Android, leading it to conclude correctly that the merger doctrine barred Oracle’s infringement claim.¹⁰⁷

A. THE FEDERAL CIRCUIT’S ANALYSIS OF THE MERGER DOCTRINE IS AT ODDS WITH *BAKER* IN THREE KEY RESPECTS

When Charles Selden devised his novel bookkeeping system, he could have designed it in a number of ways. The *Baker* Court recognized that anyone who wanted to implement the Selden system would have little choice but to select and arrange columns and headings in a substantially similar way.¹⁰⁸ Since copyright does not protect useful arts such as bookkeeping systems, but only authorial expression,¹⁰⁹ *Baker* was free to publish similar forms to instantiate the Selden system. The Court ruled that the forms were uncopyrightable.¹¹⁰ *Baker* importantly distinguished between authorship (the original expression that copyright protects) and invention (the functional creativity, which only utility patent law can protect).¹¹¹

With regard to merger, the Federal Circuit conflicts with *Baker* in three significant ways. *First*, the Federal Circuit incorrectly concluded that merger can only be found if a first author had no or only extremely limited alternative ways to express an idea when creating his work.¹¹² For example, it pointed to

106. *Id.* (emphasis added).

107. *Oracle Am., Inc. v. Google Inc.*, 872 F. Supp. 2d 974, 976 (N.D. Cal. 2012).

108. *Baker*, 101 U.S. at 101.

109. *Id.* at 101–02.

110. *Id.* at 105.

111. *Id.*

112. The Federal Circuit construed the merger doctrine inconsistently. It correctly describes the merger doctrine as applying “when there are a limited number of ways to express an idea,” *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1359 (Fed. Cir. 2014), but elsewhere it incorrectly characterized the doctrine as applying exclusively when an idea “can be expressed in only one way.” *Oracle*, 750 F.3d at 1360.

the existence of alternative names for Java functions, such as “Arith.larger” instead of “Math.max,” in finding that the merger doctrine did not apply to the Java SE declarations.¹¹³ In *Baker*, it did not matter whether column headers such as “Bro’ght Forward.” or “Distribution” could have been worded differently when implementing Selden’s accounting system.¹¹⁴

Thus, merger is a viable argument against copyrightability when the range of available alternatives for functions is limited, as the District Court concluded,¹¹⁵ and as was true in *Baker*. The District Court made a finding that there *was*, in fact, only one way to write the name of each function: “Under the rules of Java, [declarations] *must be identical* to declare a method specifying the *same* functionality—even when the implementation is different.”¹¹⁶ Thus, any programmer wishing to invoke the functionality of “Math.max” would have to use the exact phrase “Math.max.”¹¹⁷

Second, the Federal Circuit’s opinion conflicts with *Baker* in concluding that courts in merger cases can consider only constraints on the plaintiff’s creation and never constraints on the defendant’s expressive choices.¹¹⁸ The Court in *Baker* did not consider whether Selden’s own choices in designing a bookkeeping system were constrained. Nor is there anything in *Baker* suggesting that the Court rejected Selden’s copyright claim because Selden had no choice about how to select and arrange columns and headings for his bookkeeping forms. Indeed, *Baker*’s forms were somewhat different.¹¹⁹ Instead, the Court decided that once Selden designed his bookkeeping system,

113. *Id.* at 1361.

114. *See Baker Story*, *supra* note 30, at 171 (showing replica of a page from Selden’s bookkeeping form).

115. *Oracle Am., Inc. v. Google Inc.*, 872 F. Supp. 2d 974, 997 (N.D. Cal. 2012).

116. *Id.* at 976.

117. Courts since *Baker* have also concluded that merger is an available defense when there is a limited number of alternatives (and not just one choice). For example, in *Morrissey v. Procter & Gamble Co.*, the court concluded that a set of sweepstakes rules Morrissey authored was original, and that there were different ways to express the rules. 379 F.2d 675, 678 (1st Cir. 1967). However, the court noted that the range of possible expressions of sweepstakes rules admitted of little variation “so that ‘the topic necessarily requires’ if not only one form of expression, at best only a limited number, [so] to permit copyrighting would mean that a party or parties, by copyrighting a mere handful of forms, could exhaust all possibilities of future use of the substance.” *Id.* (citations omitted). The court rejected this outcome, writing that “[w]e cannot recognize copyright as a game of chess in which the public can be checkmated.” *Id.* at 679 (citing *Baker*). *Cf.* *Traffix Devices, Inc. v. Mktg. Displays, Inc.*, 532 U.S. 23, 33–34 (2001) (rejecting test for functionality of trade dress based solely on the existence of alternative designs).

118. *See Oracle*, 750 F.3d at 1361.

119. *See Baker v. Selden*, 101 U.S. 99, 101 (1880).

Baker's design choices for arranging columns and headings to implement the same system were constrained by the choices that Selden had made.¹²⁰

Third, the Federal Circuit's decision conflicts with *Baker* in holding that merger can be a defense to infringement claims, but not a basis for denying copyrightability.¹²¹ The Court in *Baker* held that Selden's forms were uncopyrightable because the selection and arrangement of columns and headings were embodiments of the bookkeeping system.¹²² Thus, the merger doctrine can be part of the copyrightability analysis and is not solely a defense to infringement.

There is a consensus among major authorities in copyright law that merger can present a copyrightability issue, not just a defense to infringement. Two major treatises now recognize that merger can serve as a bar to copyrightability.¹²³ The U.S. Copyright Office's *Compendium of U.S. Copyright Office Practices* also identifies merger as one of the bases on which the Office may refuse registration applications.¹²⁴

B. THE MERGER DOCTRINE PROVIDES A SOUND BASIS FOR HOLDING THAT PROGRAM INTERFACES THAT ENABLE COMPATIBILITY ARE UNCOPYRIGHTABLE

Since the Second Circuit's *Altai* decision, there has been broad-based consensus that computer program interfaces that enable the development of compatible software programs are not within the scope of copyright protection. Computer Associates claimed that *Altai* infringed by copying the structure of the compatibility component of its scheduling software designed

120. *Id.* More recent appellate decisions also support the idea that a first comer's choices can limit the options of those who come after. In *Veeck v. Southern Building Code Congress International, Inc.*, 293 F.3d 791 (5th Cir. 2002) (en banc), merger precluded enforcement of SBCCI's claim against Veeck for his online posting of a privately written code that had been adopted as law in Anna and Savoy, Texas. 293 F.3d at 800–02. It did not matter how many possible alternative expressions existed when the codes were initially created. *Id.* What mattered was that once enacted, there was no other way to express what the law was. *Id.* at 802.

121. *Oracle*, 750 F.3d at 1358.

122. *Baker*, 101 U.S. at 107; *see also* *Kern River Gas Transmission Co. v. Coastal Corp.*, 899 F.2d 1458, 1463–64 (5th Cir. 1990) (holding that the idea of pipeline location and its embodiment in a map are inseparable and not copyrightable); *Herbert Rosenthal Jewelry Corp. v. Kalpakian*, 446 F.2d 738, 742 (9th Cir. 1971) (citing *Baker*, 101 U.S. at 103, and concluding no copyright attached in a jeweled bee pin whose idea and expression merged).

123. *See* 1 PAUL GOLDSTEIN, GOLDSTEIN ON COPYRIGHT §§ 2.3.2, 2:38.1 (2015); 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2A.05[A][2][b] (2019).

124. *See* U.S. COPYRIGHT OFF., COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 313.3(B) (3d ed. 2015).

to run on IBM operating systems.¹²⁵ The *Altai* court invoked *Baker* as the “doctrinal starting point” of its analysis.¹²⁶

Altai articulated a three-step “abstraction, filtration, and comparison” test for judging non-literal infringement of software copyrights.¹²⁷ The first step creates a hierarchy of abstractions of the plaintiff’s program; the second step filters out unprotectable elements; and the third step compares the remaining expressive elements of the plaintiff’s program with the defendant’s program to determine if the defendant’s program is substantially similar to expressive elements copied from the plaintiff’s program.¹²⁸ Among the unprotectable elements to be filtered out are those dictated by efficiency, those constrained by external factors—such as the need to be compatible with hardware or software—and those in the public domain.¹²⁹ The court concluded that the similarities between *Altai*’s and Computer Associates’s programs were constrained by external factors, namely, the need to be compatible with IBM programs.¹³⁰

Courts have invoked the merger doctrine in concluding that even literal copying may be excused from infringement when needed to achieve compatibility.¹³¹ The Federal Circuit once recognized this principle in *Atari Games Corp. v. Nintendo of Am. Inc.*¹³² Atari Games claimed its copying of Nintendo’s data stream was necessary to enable videogames to run on its platform.¹³³ Had Atari Games copied only as much of the Nintendo data stream as was actually necessary to achieve compatibility with the then-current version of the Nintendo platform, the Federal Circuit said it would have ruled

125. *Comput. Assocs. Int’l, Inc. v. Altai, Inc.*, 982 F.2d 693, 701 (2d Cir. 1992).

126. *Id.* at 704.

127. *Id.* at 706–11.

128. *Id.*

129. *Id.* at 707–10.

130. *Id.* at 714–15.

131. The only decision—other than the Federal Circuit ruling in *Oracle*—to cast doubt on the lack of copyright protection for computer program elements required for interface compatibility was the Third Circuit’s decision in *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240 (3d Cir. 1983). Its anti-compatibility dicta should be given little weight for two reasons. First, Franklin made no effort to reimplement the interface procedures embedded in the Apple OS in independently written code. It made exact copies of the Apple programs. *Apple Computer*, 714 F.2d at 1245. Second, these statements were made at an early stage in the evolution of software copyright law, well before *Altai* and other cases described above provide more thorough analyses of the copyright implications of a second comer’s reimplementations of interface procedures necessary for interoperability.

132. 975 F.2d 832, 840 (Fed. Cir. 1992).

133. *Id.* at 836–37.

in Atari's favor on merger grounds.¹³⁴ Because it copied more than was necessary, its merger defense failed.¹³⁵

Drawing in part on *Atari Games*, the Sixth Circuit concluded that literal copying of program code to enable compatibility was justifiable under the merger doctrine in *Lexmark Int'l, Inc. v. Static Control Components, Inc.*¹³⁶ Lexmark challenged Static's copying of a program installed in Lexmark printer cartridges. Static defended by saying this copying was necessary for its chip customers to manufacture printer cartridges that interoperated with Lexmark printers.¹³⁷ There was no other way for unlicensed cartridges to perform the digital handshake with Lexmark's printer software to authenticate the cartridge so it would work in Lexmark printers.¹³⁸ The court decided that "[t]o the extent compatibility requires that a particular code sequence be included in the component device to permit its use, the merger and scenes a faire doctrines generally preclude the code sequence from obtaining copyright protection."¹³⁹

The Eleventh Circuit rendered a similar ruling in *Bateman v. Mnemonics, Inc.*¹⁴⁰ After Bateman stopped licensing the operating system on which Mnemonics had run its automated parking garage program, Mnemonics developed its own compatible operating system that reimplemented Bateman's interface.¹⁴¹ The Eleventh Circuit concluded that even literal code may be filtered out under the abstraction, filtration, and comparison test pioneered in *Altai*.¹⁴² It faulted the District Court for failing to instruct the jury "that compatibility . . . is a consideration that applies at the literal level."¹⁴³ Although the court declined to hold that interface specifications are wholly outside the scope of copyright,¹⁴⁴ it nonetheless concluded that "external considerations such as compatibility may negate a finding of infringement."¹⁴⁵ Where literal copying is "dictated by compatibility requirements,"¹⁴⁶ copyright does not apply.

These decisions affirm the conclusions of the National Commission on New Technological Uses of Copyrighted Works, whose report Congress

134. *Id.* at 839–40.

135. *Id.* at 840.

136. 387 F.3d 522 (6th Cir. 2004).

137. *Id.* at 529–30.

138. *Id.*

139. *Id.* at 536.

140. 79 F.3d 1532, 1547 (11th Cir. 1996).

141. *Id.* at 1536–37.

142. *Id.* at 1545.

143. *Id.* at 1546.

144. *Id.* at 1547.

145. *Id.*

146. *Id.*

commissioned and relied upon when regulating software copyrights.¹⁴⁷ The report explained that “[w]hen specific instructions, *even though previously copyrighted*, are the only and essential means of accomplishing a given task, their later use by another will not amount to infringement.”¹⁴⁸

C. THE FEDERAL CIRCUIT IGNORED THE DISTRICT COURT’S FACT FINDINGS THAT SUPPORTED ITS HOLDING THAT THE INTERFACES AT ISSUE WERE UNPROTECTABLE UNDER THE MERGER DOCTRINE

As these authorities demonstrate, merger is a viable argument against copyrightability when the range of available alternatives for expressing a particular idea or method is very limited. The District Court made a finding that there *was*, in fact, only one way to write the name of each function: “Under the rules of Java, [declarations] *must be identical* to declare a method specifying the *same* functionality—even when the implementation is different.”¹⁴⁹ Thus, any programmer wishing to invoke the functionality of “Math.max” would have to use the exact phrase “Math.max.”

Its conclusion that there was only one way to write the declarations is bolstered by the amicus brief submitted by 78 computer scientists.¹⁵⁰ They explain that, with a very limited exception addressed below, the Java programming language requires that declarations be written in a precise form; that reuse of software interfaces such as the Java SE declarations is a foundational practice in computer science that allows programmers to write software that performs on multiple platforms at once; and, that this reimplementing requires exact duplication of an interface’s declarations and organizational scheme.¹⁵¹

D. THE DISTRICT COURT PROPERLY HELD THAT NAMES AND SHORT PHRASES ARE NOT PROTECTABLE BY COPYRIGHT

The only part of the declarations not precisely dictated by the Java language are names given to specific functions.¹⁵² But this does not bring Oracle’s

147. NAT’L COMM’N ON NEW TECH. USES OF COPYRIGHTED WORKS, FINAL REPORT (1978).

148. *Id.* at 20 (emphasis added).

149. Oracle Am., Inc. v. Google Inc., 872 F. Supp. 2d 974, 976 (N.D. Cal. 2012).

150. See 78 Computer Scientists Cert. Brief, *supra* note 17.

151. *Id.* at 3.

152. *Id.* at 8–9.

interface within the scope of copyright. As the District Court concluded,¹⁵³ names are not protected by copyright law.¹⁵⁴

Among the circuit courts concluding that identifiers of functional items are unprotectable by copyright law is *Southco, Inc. v. Kanebridge Corp.*,¹⁵⁵ in which the Third Circuit considered whether the serial numbers used to uniquely identify hardware parts were copyrightable; it decided that they were not.¹⁵⁶ The court explained that part numbers are “excluded from copyright protection because they are analogous to short phrases or the titles of works.”¹⁵⁷

The Sixth Circuit has rendered similar rulings. In *ATC Distribution Group v. Whatever It Takes Transmissions & Parts, Inc.*,¹⁵⁸ the court held that a taxonomy for assigning unique identifiers to auto transmission parts by sorting them into categories and sub-categories was not copyrightable.¹⁵⁹ The taxonomy for assigning numbers was itself an uncopyrightable idea,¹⁶⁰ and the numbers generated through application of the taxonomy were unprotected because they were unoriginal or else merger had occurred.¹⁶¹ Beyond this, the court concluded that there were additional reasons not to grant copyright protection “to short ‘works,’ such as part numbers.”¹⁶² It recognized that allowing copyright in such short works would substantially raise the risk of litigation for those who use such works legitimately and would not meaningfully advance the progress of science and useful arts.¹⁶³ Accordingly, U.S. Copyright Office

153. *Oracle Am., Inc. v. Google Inc.*, 810 F. Supp. 2d 1002, 1009 (N.D. Cal. 2011).

154. Efficiency and other functional considerations constrain declaration names. *See* 78 Computer Scientists Cert. Brief, *supra* note 17, at 7–9.

155. 390 F.3d 276 (3d Cir. 2004) (en banc) (Alito, J.).

156. *Id.* at 277–78.

157. *Id.* at 285. The Court also held that the serial numbers were not original expressions. *Id.* at 282.

158. 402 F.3d 700 (6th Cir. 2005).

159. *Id.* at 706.

160. *Id.* at 707.

161. *Id.*

162. *Id.* at 709.

163. *Id.* at 709–10; *see also* *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 542 (6th Cir. 2004) (invoking the names and short phrases doctrine to reject Lexmark’s claim that inserting stock ticker symbols into code was creative expression). Other circuits have denied copyright protection to names on other grounds. *See, e.g., Mitel, Inc. v. Iqtel, Inc.*, 124 F.3d 1366, 1373 (10th Cir. 1997) (holding four-digit numeric codes used to access features of telecommunications hardware were not copyrightable due to unoriginality and *scènes à faire*).

procedures recognize that “[w]ords and short phrases such as *names*, titles, and slogans” are not copyright-protectable.¹⁶⁴

The only parts of the declaration that are not precisely dictated by the Java programming language are names, and they too are unprotectable. Thus, no aspect of the declarations is protectable by copyright law.

IV. CONCLUSION

This Article, drawn from our brief amicus curiae in support of the Petitioner in *Google v. Oracle*, offers an analysis of the scope of software copyright law that is consistent with the most pertinent Supreme Court precedents, case law decided both before and after the 1976 Act, and the text of the § 102(b) exclusions of methods and systems from copyright’s scope. The Oracle brief ignored almost all of the decisions we rely upon and ignored all but one of the § 102(b) exclusions.¹⁶⁵ The danger of excessively broad copyright protection for computer programs, which prompted Congress to add these exclusions to the statute, is posed by this case. As the amicus curiae briefs of 83 computer scientists, IBM Corp., Microsoft, the Developers Alliance,¹⁶⁶ among others, explained, the Court’s decision in *Google v. Oracle* will have profound effects on the software industry. No wonder the case was called the “copyright case of the century.”¹⁶⁷

164. 37 C.F.R. § 202.1(a) (emphasis added). The Copyright Office’s Circular 34, *Copyright Protection Not Available for Names, Titles, or Short Phrases*, was updated to become Circular 33, *Works Not Protected by Copyright*, available at <https://www.copyright.gov/circs/circ33.pdf>. The update is noted in the Office’s Circular Update Guide, <https://www.copyright.gov/circs/circular-update-guide.pdf>.

165. Brief for Respondent, *Google LLC v. Oracle Am., Inc.*, No. 18-956 (U.S. Feb. 12, 2020).

166. Amicus briefs in support of petitioner Google filed by 83 Computer Scientists, International Business Machines Corp. et al., Microsoft Corp., and Developers Alliance, along with other submissions in the *Google v. Oracle* case, can be found on the U.S. Supreme Court site: <https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/18-956.html>.

167. See, e.g., Scott Graham, *Supreme Court, Finally, Takes Up ‘Google v. Oracle,’* LAW.COM (Nov. 15, 2019), <https://www.law.com/nationallawjournal/2019/11/15/supreme-court-finally-takes-up-google-v-oracle/?slreturn=20200124134715> (quoting Professor Mark Lemley).

TRADEMARKS AS SURVEILLANCE TRANSPARENCY

Amanda Levendowski[†]

ABSTRACT

We know very little about the technologies that watch us. From cell site simulators to predictive policing algorithms, the lack of transparency around surveillance technologies makes it difficult for the public to engage in meaningful oversight. Legal scholars have critiqued various corporate and law enforcement justifications for surveillance opacity, including contract and intellectual property law. But the public needs a free, public, and easily accessible source of information about corporate technologies that might be used to watch us. To date, the literature has overlooked a free, extensive, and easily accessible source of information about surveillance technologies hidden in plain sight: federal trademark filings.

This Essay examines the powerful and unexplored role of trademark law in exercising oversight within and beyond surveillance. Trademark law promotes access to information, and the process for federal registration of trademarks—long overlooked by scholars—demands extensive public disclosures that reveal a wealth of information about surveillance technologies. This Essay leverages examples from real trademark applications to explore how journalists, researchers, and civil society can use the detailed disclosures in trademark applications for transparency. I conclude that trademark law can be a powerful tool for correcting longstanding information asymmetries between the watchers and the watched by empowering the public to watch back.

DOI: <https://doi.org/10.15779/Z38VT1GQ6P>

© 2021 Amanda Levendowski.

[†] Associate Professor of Law, Georgetown University Law Center. Thanks to Lindsey Barrett, Barton Beebe, Hannah Bloch-Wehba, Priya Chadha, Julie Cohen, Bradley Girard, Dave Gershorn, Thomas Haley, Alex Reeve Givens, Megan Graham, Woody Hartzog, Brett Max Kaufman, Christina Koningisor, Marty Lederman, Karen Levy, Naomi Mezey, Mark McKenna, Chris Morten, Laura Moy, Jennifer Rothman, Matthew Sag, Madelyn Sanfillipio, Jessica Silbey, Ed Timberlake, Rebecca Tushnet, Jacob Victor, Ari Waldman, Rebecca Wexler, and Cameron Tepski for their thoughtful and generous comments. This Essay benefited from presentation at the Georgetown Tech Law Scholar Seminar, Privacy Law Scholars Conference, Junior Law and Tech* Scholars Workshop, and Georgetown Faculty Workshop. Shadé Oladetimi provided sharp research assistance.

TABLE OF CONTENTS

| | | |
|-------------|---|------------|
| I. | INTRODUCTION | 440 |
| II. | DISCOVERING DISCLOSURES IN TRADEMARK FILINGS | 445 |
| | A. INTENT TO USE OR IN-USE DESIGNATION | 448 |
| | B. GOODS AND SERVICES CLASSIFICATIONS AND DESCRIPTIONS | 449 |
| | C. SPECIMENS..... | 451 |
| III. | REVEALING DISCLOSURES IN TRADEMARK FILINGS FOR SURVEILLANCE TECHNOLOGIES | 452 |
| | A. STINGRAY: CELL-SITE LOCATION INFORMATION INTERCEPTORS | 453 |
| | B. VIGILANT SOLUTIONS: AUTOMATED LICENSE PLATE READERS | 457 |
| | C. PREDPOL: PREDICTIVE POLICING ALGORITHMS | 463 |
| IV. | CONCLUSION..... | 468 |

I. INTRODUCTION

In February 2018, Amazon acquired a “smart” doorbell company called Ring.¹ For Amazon, a company that delivers more than 5 billion items annually,² acquiring a way to monitor the real estate where packages get delivered makes sense. Yet statements from the acquired Ring seemed grandiose for the purchase of a private security system, including that the company “look[ed] forward to being a part of the Amazon team as we work toward our vision for safer neighborhoods.”³ Amazon’s full vision for Amazon Ring devices became clear to the public more than a year later when journalists revealed that the company had quietly partnered with police departments

1. Laura Stevens & Douglas MacMillan, *Amazon Acquires Ring, Maker of Video Doorbells*, WALL ST. J. (Feb. 27, 2018), <https://www.wsj.com/articles/amazon-acquires-ring-maker-of-video-doorbells-1519768639>.

2. Ashley Carman, *Amazon Shipped over 5 Billion Items Worldwide Through Prime in 2017*, THE VERGE (Jan. 2, 2018), <https://www.theverge.com/2018/1/2/16841786/amazon-prime-2017-users-ship-five-billion>.

3. Eugene Kim, *Amazon Buys Smart Doorbell Maker Ring for a Reported \$1 Billion*, CNBC (Feb. 27, 2018), <https://www.cnbc.com/2018/02/27/amazon-buys-ring-the-smart-doorbell-maker-it-backed-through-alexa-fund.html>.

across the country to promote and deploy Amazon Ring devices as part of a privatized surveillance network.⁴

Private companies, like Amazon, increasingly create surveillance technology used by law enforcement, but the public is often not aware that these technologies are being developed and deployed until the technology is already embedded in communities. Private companies developing surveillance technology for law enforcement is not new, and neither is the lack of transparency around those relationships. Acquisitions of surveillance technology may be made with outside funding or through in-kind donations to police departments, making surveillance technology difficult to track through financial disclosures.⁵ Filing federal Freedom of Information Act (FOIA) requests or using local public records laws to ask for information about surveillance technologies used by law enforcement is, as Hannah Bloch-Wehba has highlighted, resource intensive and lacks any guarantee that law enforcement will disclose responsive documents about surveillance technology.⁶ Elizabeth Joh has detailed how private contracts, such as non-

4. Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, MOTHERBOARD (July 25, 2019), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement; Dell Cameron, *Amazon's Ring Barred Cops From Using 'Surveillance' to Describe Its Products*, GIZMODO (Aug. 19, 2019), <https://gizmodo.com/ring-barred-cops-from-using-surveillance-to-describe-it-1837380102>; Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?noredirect=on>. Earlier this year, the House Subcommittee on Economic and Consumer Policy sent a letter to Amazon requesting detailed information about partnerships between Amazon Ring and law enforcement. See Letter from Raja Krishnamoorthi, Chairman, H. Subcomm. on Econ. & Consumer Pol., to Brian Huseman, Vice President of Pub. Pol'y, Amazon.com, Inc. (Feb. 19, 2020), <https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2020-02-19.RK%20to%20Huseman-Amazon%20re%20Ring%20%281%29.pdf>.

5. Laura Nahmais, *Police Foundation Remains a Blind Spot in NYPD Contracting Process, Critics Say*, POLITICO (July 13, 2017), <https://www.politico.com/states/new-york/city-hall/story/2017/07/13/police-foundation-remains-a-blind-spot-in-nypd-contracting-process-critics-say-113361>. Thanks to Rashida Richardson for this observation.

6. Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1296–1303 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355776; see also, Order denying permissibility of Glomar response with regard to documents requested by protestors, *Millions March NYC v. N.Y. City Police Dep't*, Index No. 100690 (Jan. 14, 2019), <https://assets.documentcloud.org/documents/5684730/Nypd-Foil.pdf> (denying New York City Police Department's Glomar response withholding responsive documents regarding surveillance technology used during protests); *infra* Part II. For a thorough examination of the shortcomings of FOIA requests, see generally Nathan Freed Wessler, “[We] Can Neither Confirm Nor Deny the Existence or Nonexistence of Records Responsive to Your Request”: Reforming the Glomar Response to FOIA, 85 N.Y.U. L. REV. 1381 (2010).

disclosure agreements between police departments and surveillance technology companies, can pose another roadblock to transparency.⁷ And Rebecca Wexler and Sonia Katyal have likewise documented the ways in which trade secret law can operate to shield surveillance technology from public scrutiny.⁸ Some jurisdictions have responded to this disparity by enacting procurement policies for surveillance technologies, as Catherine Crump has examined, but few jurisdictions have enacted policies that require public disclosure of a proposed surveillance technology prior to procurement.⁹ Taken together and put into practice, these hurdles look like invoking non-disclosure agreements to avoid judicial scrutiny of surveillance technology,¹⁰ incentivizing companies to collect and sell personal information without consent or notice,¹¹ and shielding surveillance algorithms from independent review or oversight.¹² The reasons vary, but the result is the same: there is a vast informational inequity between law enforcement and the public about surveillance technologies.¹³

Journalists and civil society have turned to other public sources of information, such as Securities and Exchange Commission disclosures and patent filings, to help correct these disparities.¹⁴ But SEC disclosures are often too general to reveal useful information about surveillance technology products.¹⁵ And patent filings are not a promise to produce a product, as

7. Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. 101 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2924620.

8. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920883; Sonia Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3409578.

9. Catherine Crump, *Surveillance Policy Making by Procurement*, 90 WASH. L. REV. 1596 (2016), <https://scholarship.law.berkeley.edu/facpubs/2633/>; see also Ira Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961 (2018), <https://digitalcommons.law.uw.edu/wlr/vol93/iss4/8/> (discussing procurement policies in Seattle, Washington and New York, New York).

10. See *infra* Part III.A (discussing Harris Corporation's Stingray devices).

11. See *infra* Part III.B (discussing Vigilant Solutions' automated license plate readers).

12. See *infra* Part III.C (discussing PredPol's predictive policing algorithms).

13. See *infra* Part III (discussing asymmetries between public awareness of law enforcement surveillance technologies and law enforcement's use of those technologies).

14. See, e.g., AMAZON, ANNUAL REPORT (FORM 10-K) 51–2 (Dec. 31, 2018), <https://www.sec.gov/Archives/edgar/data/1018724/000101872419000004/amzn-20181231x10k.htm> (using K-filings to investigate Amazon); Generating Composite Facial Images Using Audio/Video Recording and Communications Devices, U.S. Patent Application No. 15/984,298, Publication No. 20180341835 (published Nov. 29, 2018) (Amazon Technologies, Inc., applicant), https://www.aclunc.org/docs/Amazon_Patent.pdf (using patent filings to investigate Amazon).

15. See, e.g., AMAZON, *supra* note 14, at 51–2 (disclosing that Ring Inc. was purchased “for cash consideration of approximately \$839 million” for the primary reason, along with

Amazon pointed out when confronted with a patent filing for a Ring-compatible expansion that would enable the cameras to create composite images of people to incorporate into a “database of suspicious persons.”¹⁶

Taken together, surveillance transparency has never been more challenging. If there is hope for resistance—including public discussion or dialogue—before law enforcement embraces secret surveillance technologies, the public desperately needs a freely available, easily accessible source of information about the technologies that will be used to watch us.¹⁷ One source is consistently overlooked: federal trademark filings.

Take Amazon Ring. In its August 2018 trademark application for the AMAZON RING mark, Amazon publicly revealed its vision for Ring: “[a]utomated self-contained electronic surveillance that can be deployed to

other acquisitions, of “acquir[ing] technologies and know-how to enable Amazon to serve customers more effectively”).

16. Generating Composite Facial Images Using Audio/Video Recording and Communications Devices, U.S. Patent Application No. 15/984,298, Publication No. 20180341835 (Published Nov. 29, 2018) (Amazon Technologies, Inc., applicant), https://www.aclunc.org/docs/Amazon_Patent.pdf; see also Peter Holley, *This Patent Shows Amazon May Seek to Create a Database of Suspicious Persons’ Using Facial-Recognition Technology*, WASH. POST, (Dec. 18, 2018), <https://www.washingtonpost.com/technology/2018/12/13/this-patent-shows-amazon-may-seek-create-database-suspicious-persons-using-facial-recognition-technology/>; Jacob Snow, *Amazon’s Disturbing Plan to Add Face Surveillance to Your Front Door*, ACLU: SPEAK FREELY BLOG, (Dec. 12, 2018), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-disturbing-plan-add-face-surveillance-yo-0>. For an accounting of why technology companies continue to file for dystopian patents, see generally Janet Freilich, *Prophetic Patents*, 53 U.C. DAVIS L. REV. 663 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202493 (examining patents that contain fictional data); Rose Eveleth, *Why Are There So Many Weird Tech Patents?*, SLATE, (Aug. 28, 2019), <https://slate.com/technology/2019/08/amazon-sony-facebook-strange-patents.html> (assessing the incentives that fuel hypothetical patents).

17. Surveillance technology is disproportionately deployed against people with limited political power. For a detailed accounting of the ways in which U.S. surveillance is deeply rooted in anti-Blackness, see generally SIMONE BROWNE, *DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS* (2015). American surveillance expanded quickly to include many other marginalized people, including immigrants, religious minorities, and poor and working people. For an accounting of how past and present practices of the American law enforcement surveillance apparatus affect each in turn, see generally GEORGETOWN LAW: CENTER FOR PRIVACY AND TECHNOLOGY, *COLOR OF SURVEILLANCE*, <https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2017> (last visited Nov. 19, 2020).

gather evidence or intelligence.”¹⁸ And it did so nearly a year before journalists detailed how that vision would operate in practice.¹⁹

Federal trademark filings can offer important insight into the surveillance technologies that private corporations are developing, but the public has not fully explored the Trademark Electronic Search System (TESS) and Trademark Status and Document Retrieval (TSDR) databases as joint pathways toward surveillance transparency.²⁰ The reason is obvious. As Justice Samuel Alito observed, “[I]t is unlikely that more than a tiny fraction of the public has any idea what federal registration of a trademark means.”²¹

This is, in some part, attributable to the dearth of scholarly writing related to the federal trademark registration process. As recently as 2017, Rebecca Tushnet observed that the mechanics of trademark registration garner little attention—and not much has changed in the interim years.²² This Essay delves

18. AMAZON RING, U.S. Trademark Application Serial No. 88075713, TEAS RF New Application at 5 (filed Aug. 13, 2018).

19. Compare Amanda Levendowski, *How Can We Learn About the AI Systems That Might Be Used to Surveil Us? The Federal Trademark Register Has Answers*, AI ETHICS INITIATIVE: GUEST BLOGGER (Oct. 11, 2018), <https://aiethicsinitiative.org/news/2018/10/11/guest-blogger-amanda-levendowski-how-can-we-learn-about-the-ai-systems-that-might-be-used-to-surveil-us-the-federal-trademark-register-has-answers> (published less than a month after the trademark application for the AMAZON RING mark was filed), with Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, VICE MOTHERBOARD (July 25, 2019), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement (revealing program discovered via public records requests requiring local law enforcement to “[e]ngage the Lakeland community with outreach efforts on the platform to encourage adoption of the platform/app”), and Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach> (detailing hundreds of partnerships between Amazon Ring and local law enforcement offering discounts to cities and community groups that invest public or taxpayer-supported funds on Amazon Ring devices and potentially grant access to civilians’ home devices).

20. There are also 50 state trademark registers, each with their own rules and procedures and processes, and international registers, some of which are accessible online. See, e.g., *eSearch Plus*, EUR. UNION INTELL. PROP. OFF., <https://euipo.europa.eu/eSearch/> (last visited Jan. 5, 2020) (search database for European Union trademarks, designs, owners, representatives, Bulletins, and Office decisions); *TMview*, EUR. UNION INTELL. PROP. OFF., <https://www.tmdn.org/tmview/welcome> (last visited Jan. 5, 2020) (database of trademark names, applications, and registration numbers in additional countries and databases).

21. *Matal v. Tam*, 137 S. Ct. 1744, 1759 (2017) (citing Application of Nat’l Distillers & Chem. Corp. 49 C.C.P.A. 854, 863 (1962) (Rich, J., concurring)).

22. Rebecca Tushnet, *Registering Disagreement: Registration in Modern American Trademark Law*, 130 HARV. L. REV. 867, 870–71 (2017), <http://harvardlawreview.org/wp-content/uploads/2017/01/867-941-Online-updated.pdf> (“Foundational critiques of modern trademark law tend not to address the role of registration. . . . Proponents of the Chicago School of law and economics approach, whose account of the function of trademark as

into the largely unexamined mechanics of the federal trademark registration process and analyzes how the process of federally registering trademarks compels companies to disclose details about new surveillance technologies. In so doing, this Essay's goal is to offer a new tool in the quest for surveillance transparency and to equip the public, including journalists, researchers, and civil society, with the skills necessary to investigate trademark records for themselves.

The Essay proceeds in two parts. Part II describes the process for federal registration of trademarks and identifies three portions of trademark filings that are likely to disclose information about surveillance technology: the stated basis for use, the goods and services description, and the specimen. Part III uses the applications for registration of trademarks for three surveillance technologies—Harris Corporation's STINGRAY cell site location information (CSLI) interceptor, Vigilant Solution's VIGILANT SOLUTIONS automated license plate reader, and Predpol's PREDPOL predictive policing software—to illustrate how to leverage revealing disclosures in trademark filings for transparency. This Essay concludes that federal trademark filings are a freely available, easily accessible way for the public to learn about surveillance technologies used to watch us.

II. DISCOVERING DISCLOSURES IN TRADEMARK FILINGS

A trademark is “any word, name, symbol, device, or any combination” of those things that can be used to identify the provider or seller, and indicate the source, of certain goods and services.²³ As the Supreme Court has observed, “[f]ederal law does not create trademarks.”²⁴ Rather, it is the seller's use of a mark that creates a trademark which grants some enforceable rights.²⁵ The reality remains, however, that federal trademark registration confers crucial rights and benefits, such as providing constructive notice of the registrant's

reducing consumers' search costs is now dominant, likewise have little to say about registration. . . . American scholars, in sum, have often treated registration like a borrowed civil law coat thrown awkwardly over the shoulders of a common law regime.”)

23. *Trademark Basics*, U.S. PAT. & TRADEMARK OFF., <https://www.uspto.gov/trademarks-getting-started/trademark-basics> (last visited Sept. 22, 2019).

24. *Matal*, 137 S. Ct. at 1751 (quoting *Be&B Hardware, Inc. v. Hargis Indus.*, 575 U.S. 138, 142 (2015)).

25. *See, e.g.*, 15 U.S.C. § 1125 (protecting qualifying unregistered marks from infringement, dilution, and tarnishment); *see also* 15 U.S.C. § 1125(d) (protecting qualifying unregistered marks from cybersquatting).

claim of ownership and offering prima facie evidence that the registered mark is valid.²⁶

There is ample scholarship exploring the purposes of trademark law.²⁷ But as Rebecca Tushnet has explained, precious little of that scholarship details the mechanics of federal trademark registration.²⁸ Indeed, to date, there has been no scholarship centered on the mechanics of investigating federal trademark filings.

The federal trademark registration process begins, somewhat circuitously, with an application to register a trademark.²⁹ An applicant discloses detailed information about the mark they are seeking to register, including whether the mark has been used, the sorts of goods and services on which the mark is (or will be) used, and, in some instances, a depiction of how the mark is (or will be) used in the real world.³⁰ Federal trademark filings are all freely and publicly

26. *Matal*, 137 S. Ct. at 1753 (quoting *B&B Hardware*, 575 U.S. 138, 142) (detailing additional benefits of federal registration). Owners of a federally registered trademark can also prevent importation of items bearing an infringing mark into the United States. *See* 15 U.S.C. § 1124. The tremendous value of a trademark registration explains why, despite having to reveal information about secretive surveillance technologies, companies continue to seek federal trademark registrations for their marks.

27. *See, e.g.*, William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 J. LAW & ECON. 265, 296 (1987) (advocating an economic theory of trademark law); Barton Beebe, *The Semiotic Analysis of Trademark Law*, 51 UCLA L. REV. 621, 669 (2004) (advancing a semiotic theory underlying trademark law); Mark P. McKenna, *The Normative Foundations of Trademark Law*, 82 NOTRE DAME L. REV. 1839 (2007) (examining multiple theories of trademark law, including preventing trade diversion, protecting consumers, and the shift toward protecting marks qua marks).

28. *See* Rebecca Tushnet, *Registering Disagreement: Registration in Modern American Trademark Law*, 130 HARV. L. REV. 867, 870–71 (2017).

29. *See* *Kelly Servs. v. Creative Harbor, LLC*, 846 F.3d 857, 876 (6th Cir. 2017) (Batchelder, J., dissenting), <https://www.leagle.com/decision/infco20170123094> (providing perhaps the most complete judicial discussion of the trademark application and registration process).

30. *See generally*, *Apply Online*, U.S. PAT. & TRADEMARK OFF., <https://www.uspto.gov/trademarks-application-process/filing-online> (last visited Nov. 20, 2020) (outlining the forms necessary to apply for a federal trademark online). The revealing disclosures demanded by the federal trademark application process incentivize some companies to take advantage of the closed, non-public registers of countries like Trinidad and Tobago—or to use shell companies, as was the case with the AMAZON RING filing—to protect their mark without disclosing detailed information to the public about products or services in development. *See* AMAZON RING, U.S. Trademark Application Serial No. 88075713 (filed on Aug. 13, 2018 by “A9.com, Inc.” and later assigned to Amazon Technologies, Inc. on May 15, 2019). These methods allow a company to claim priority of the earlier foreign filing without disclosing details about the mark—or the mark itself—until months later. For a detailed analysis of these so-called “submarine trademarks,” *see generally* CARSTEN FINK, ANDREA FOSFURI, CHRISTIAN HELMERS & AMANDA MYERS, *Submarine Trademarks*, NORTHWESTERN PRITZKER SCHOOL OF

searchable using the TESS. The U.S. Patent and Trademark Office (USPTO) launched TESS in 2000.³¹ TESS offers a way to search federal trademark filings online without cost but, while it does not require any technical expertise, it can be a tricky interface.

There are two primary types of TESS searches: simple and structured.³² Using the basic fields in both types of searches, enquirers can surface trademark applications for surveillance technologies through strategic queries. Simple searches enable searching by limited criteria, namely by Combined Word Mark (e.g., AMAZON RING), Serial or Registration Number (88075713), and Owner Name and Address (Amazon Technologies, Inc., 410 Terry Avenue North, Seattle, Washington 98109).³³ Structured searches permit searching by a wider range of search terms across many more fields, including Current Basis (1B, Intent to Use), Goods and Services (surveillance), and International Class (Class 9).³⁴ After running a search using TESS, one can view each of the filings for a particular application for registration of a trademark using the TSDR system.³⁵

Crucially, and unlike patent applicants, all federal trademark applicants must make “bona fide use of the mark in the ordinary course of trade, and not made merely to reserve a right in a mark” before the Examiner will allow a mark to be added to the Principal or Supplemental Register.³⁶ Applicants who make misrepresentations during the trademark application process risk losing

LAW (Feb. 15, 2019), http://www.law.northwestern.edu/research-faculty/clbe/events/innovation/documents/helmets_submarine_trademarks.pdf.

31. USPTO *Introduces New Trademark Electronic Search System*, U.S. PAT. & TRADEMARK OFF., <https://www.uspto.gov/about-us/news-updates/uspto-introduces-new-trademark-electronic-search-system> (last visited Oct. 22, 2019); *see also* Barton Beebe & Jeanne C. Fromer, *Are We Running Out of Trademarks? An Empirical Study of Trademark Depletion and Congestion*, 131 Harv. L. Rev. 945, 970–71 (2018) (discussing the origins of TESS).

32. *Trademark Electronic Search System*, U.S. PAT. & TRADEMARK OFF., <http://tmssearch.uspto.gov>. (last visited Oct. 22, 2019). The third type of search, free form, permits the construction of searches using Boolean logic across multiple search fields. *See id.*

33. *Id.*

34. *Id.*; *see infra* Parts II.A–C.

35. There are many acronyms involved in the process to federally register a trademark. *See Trademark Status and Document Retrieval (TSDR)*, U.S. PAT. & TRADEMARK OFF., <http://tsdr.uspto.gov/>. Note that there are far fewer ways to run trademark searches using TSDR, which limits search fields to US Serial, Registration, or Reference number or International Registration number. *Id.*

36. 15 U.S.C. § 1127; *see also* U.S. PAT. & TRADEMARK OFF., TRADEMARK MANUAL OF EXAMINING PROCEDURE § 901.02 (Oct. 2018), <https://tmep.uspto.gov/RDMS/TMEP/current#/Oct2018/TMEP-900d1e7.html> [hereinafter TMEP]. Note that there are special provisions for marks registered internationally. *See, e.g.*, 15 U.S.C. § 1126; 15 U.S.C. § 1141(f).

federal trademark protection for their mark.³⁷ Requiring that applicants must intend to use the mark in connection with the goods and services identified in the application for registration means that applications for registration of trademarks avoids the issue created by dystopian patents that companies, like Amazon, dismiss as speculative.³⁸ Instead, the bona fide requirement forces companies to stand by representations made in their applications, correct their errors or admit to misleading the USPTO.

Three portions of the applications to register trademarks predictably yield useful information about surveillance technologies. The first is the “use designation,” which requires the applicant to identify whether the application for registration is based on use of the mark for the underlying product or whether the application is based on an intent to use the mark.³⁹ The second is the goods and services classifications and descriptions, which offer general categorizations and specific identifications of the types of products for which the mark will be used. And the final one, and perhaps the most unique and valuable, is the “specimen” portion, which consists of visual representations depicting how the mark is used in commerce—think screenshots of computer interfaces and photographs of hardware emblazoned with logos. This Part examines each of those three portions of trademark applications in turn.

A. INTENT TO USE OR IN-USE DESIGNATION

Federal trademark filings require a designation regarding whether the owner currently uses the mark in commerce or whether the owner intends to use the mark at a future date.⁴⁰ When viewing an application in TESS, these designations are coded as filing bases 1A and 1B, respectively.⁴¹ For in-use applications, the owner must disclose the date the mark was first used in commerce.⁴² The use designation offers a way to determine when goods and

37. *See, e.g.*, *Nationstar Mortgage LLC v. Ahmad*, 112 U.S.P.Q.2d 1361 (T.T.A.B. 2014) (sustaining fraud claim and refusing to register NATIONSTAR mark).

38. *See supra* Part I.

39. The mark need not be in use at the time of the filing, so long as the use designation is identified as “intent-to-use.” *See* TMEP, *supra* note 36, § 1101.

40. 15 U.S.C. § 1051(a)–(b).

41. The 1A and 1B designations are named after the sections of the Lanham Act that govern federal trademark applications. *See* 15 U.S.C. § 1051(a)–(b). The intent-to-use designation was introduced by the Trademark Law Revision Act of 1988. Pub. L. No. 100-667, 15 U.S.C. § 1051(b) (1988). For skepticism about whether intent-to-use applications were an ill-advised addition to the Lanham Act, see generally Amy B. Cohen, *Intent to Use: A Failed Experiment?*, 35 U.S.F. L. REV. 683 (2001).

42. 15 U.S.C. § 1051(a)(2). Six months after filing an intent-to-use application, the owner must file a Statement of Use confirming that the mark is being used in commerce or risk abandoning the application. 15 U.S.C. § 1051(d)(1). On a showing of good cause by the applicant, the Director of the U.S. Patent and Trademark Office may grant a series of six-

services under a particular mark were first offered to the relevant purchasing public, which, in some instances, may be sales to law enforcement.

B. GOODS AND SERVICES CLASSIFICATIONS AND DESCRIPTIONS

The goods and services classification and description portion of federal trademark filings consists of two components: a numerical classification categorizing the goods or services and a plain-language description of the goods or services to be covered by a particular mark.⁴³ The classification and description requirement for federal trademark filings dates back to 1870 and the earliest codified trademark law in the United States, which required applicants to identify “the class of merchandise and the particular description of goods comprised in such class, by which the trademark has been or is intended to be appropriated.”⁴⁴ Subsequent trademark laws similarly required the identification of goods, although without acknowledging protection for federal trademarks used in connection with services.⁴⁵ The Lanham Act, passed in 1946, finally extended trademark protection to services.⁴⁶

Federal law does not mandate a classification system, but the Director of the USPTO has determined one:⁴⁷ the Nice Classification, a numerical classification system featuring 45 distinct classes, with so-called International Classes 1 through 34 identifying goods and International Classes 35 through

month extensions, so long as the overall extension does not exceed 24 months. 15 U.S.C. § 1051(d)(2); *Trademark Applications—intent-to-use (ITU) basis*, U.S. PAT & TRADEMARK OFF., <https://www.uspto.gov/trademarks-application-process/filing-online/intent-use-itu-applications> (last visited Nov. 30, 2020).

43. See TMEP, *supra* note 36, 1401.02(a).

44. The Act ironically made no mention of trademark in its title but was rather intended to “revise, consolidate, and amend the statutes relating to patents and copyrights.” H.R. 1714, 41st Cong. (1870). The first U.S. trademark law was struck down as unconstitutional after *The Trade-Mark Cases* in 1879, when the Supreme Court held that the Copyright Clause of the Constitution did not give Congress the power to protect or regulate trademarks. See *The Trade-Mark Cases*, 100 U.S. 82 (1879). Subsequent trademark laws were enacted under the authority of the Commerce Clause. See TMEP, *supra* note 36, § 1401.02(a).

45. See, e.g., 1881 Trademark Bill; H.R. 16560, 58th Cong. (1905) (authorizing the registration of trademarks).

46. See Lanham Act of 1946, ch. 540, 60 Stat. 427; see also *In re Dr. Pepper Co.*, 836 F.2d 508, 509 (Fed. Cir. 1987) (holding a contest to promote the sale of one’s goods is not a “service” within the meaning of the Latham Act).

47. 15 U.S.C. § 1112; TMEP, *supra* note 36, § 1401.02(a). Classifications are also the primary basis for determining registration fees for federal trademark applications, with each class costing between \$225 and \$400 depending on the type of trademark application. *Overview of Trademark Fees*, U.S. PAT. & TRADEMARK OFF., <https://www.uspto.gov/trademark/fees-payment-information/overview-trademark-fees> (last visited Oct. 28, 2019); TMEP, *supra* note 36, § 1401.01.

45 identifying services.⁴⁸ Class 1, for example, covers “chemicals,” including those used in industry, science, photography, agriculture, and forestry, among many others.⁴⁹

Surveillance technologies are likely to fall into one or more of the following classes: Class 9 covering electrical and scientific apparatuses, which includes hardware and computer software (such as body-worn cameras⁵⁰ or predictive policing algorithms), Class 42 covering computer and scientific services (such as developing big data analytics software), or Class 45 covering personal and legal services (such as surveillance services or monitoring computer services for clients).⁵¹ Goods and services descriptions offer additional detail about the goods or services on which a mark will be used. Many model goods and services descriptions are included in the Acceptable Identification of Goods and Services Manual (ID Manual),⁵² which operates as a guide for trademark applicants looking to craft goods and services descriptions that will be intelligible to trademark examiners and thus unlikely to create complications for the application.⁵³ Applicants may try to disclose limited information in goods and services descriptions, but such strategies may limit the power of the

48. TMEP, *supra* note 36, § 1401.02(a); *see also* the Nice Agreement (establishing a classification of goods and services for purposes of registering trademarks and service marks). The United States became a signatory to the Nice Agreement in 1973. *See* TMEP, *supra* note 36, § 1401.02(a).

49. TMEP, *supra* note 36, § 1401.02(a).

50. Taser International filed a trademark application for the AXON AI mark covering “[s]urveillance services featuring use of video cameras that can be worn on the head and the body and video surveillance systems used in automobiles, and computers and mobile electronic devices to provide location-specific information about the video” on February 20, 2017—more than 40 days before the rebrand from Taser to Axon was made public, teasing the company’s increasing focus on software rather than hardware. *Compare* AXON AI, U.S. Trademark Application Serial No. 87341984 (filed Feb. 20, 2017), *with* Stephen Nellis, *Taser Changes Name to Axon in Shift to Software Services*, REUTERS (Apr. 5, 2017), <https://www.reuters.com/article/us-usa-taser/taser-changes-name-to-axon-in-shift-to-software-services-idUSKBN177265>.

51. TMEP, *supra* note 36, § 1401.02 (a). Other possible, though less likely, classes for surveillance technologies include Class 35 covering advertising and business services, Class 38 covering telecommunications services, and Class 41 covering education and entertainment services. *Id.*

52. *See Trademark ID Manual, ID Master List*, U.S. PAT. & TRADEMARK OFF., <https://idm-tmng.uspto.gov/id-master-list-public.html> (last visited Oct. 10, 2019). The ID Manual can be used to identify how particular goods and services related to surveillance are likely to be phrased. Those phrases can then be searched using TESS.

53. TMEP, *supra* note 36, § 1402.04. Applicants may create their own goods and services descriptions, but trademark examiners may take issue with the specificity of the description or disagree that a particular description is consistent with the identified class. In that case, the examiner may issue an “Office Action” to the applicant suggesting revisions to the existing description or requesting revisions from the applicant. *See* TMEP, *supra* note 36, § 705.

mark and, in some instances, trigger Office Action requests from the Examiner seeking information about additional goods and services.⁵⁴

Searches using classifications and goods and services descriptions are “structured” searches within TESS.⁵⁵ After selecting the option to begin a structured search, users can search by classification by typing the desired class number as the “Search Term” and selecting “International Class” as the field.⁵⁶ Because a search premised on class alone would likely return many irrelevant results, one can further filter the search by typing key words from the goods and services description, such as “surveillance,” as the Search Term and selecting “Goods & Services” as the field.⁵⁷ This search method is likely to yield surveillance technologies that may be used by law enforcement, such as the AMAZON RING application.⁵⁸

C. SPECIMENS

Trademark applications filed on an in-use basis must include a “specimen,” meaning some kind of label, tag, packaging, or other display that shows the mark used in connection with every class described in the application.⁵⁹ Specimens are required because they “... show the manner in which the mark is seen by the public . . . [and] provide supporting evidence of facts recited in

54. See generally TMEP, *supra* note 36, § 705.

55. See *Trademark Electronic Search System (TESS)*, U.S. PAT. & TRADEMARK OFF., <http://tmsearch.uspto.gov> (last visited Oct. 10, 2019).

56. *Trademark Electronic Search System (TESS) Structured Search*, U.S. PAT. & TRADEMARK OFF., <http://tmsearch.uspto.gov> (last visited Oct. 10, 2019). Classes must be stylized to three digits, such that a search for Class 9 would require entering “009” as the Search Term. *Id.*

57. *Trademark Electronic Search System (TESS) Structured Search*, U.S. PAT. & TRADEMARK OFF., <http://tmsearch.uspto.gov> (last visited Oct. 10, 2019). I am working with a Georgetown Law student to create a tool that automates this process and generates an update when a trademark application containing “surveillance” in the goods and services description is filed.

58. See AMAZON RING, Registration No. 88075713, (covering, in part, “security surveillance apparatus, namely, electronic components of security systems,” “software development kits (SDKs) comprising of software development tools and software for use as an application programming interface (API) for creating software and applications related to theft-prevention and security systems, and home and business surveillance systems,” “electronic video surveillance products, namely, electronic components of security systems; global positioning navigation software for use with smart, autonomous vehicles and mobile machines for use in connection with internet of things (IoT) enabled devices,” and “Automated self-contained electronic surveillance devices that can be deployed to gather evidence or intelligence,” all in Class 9).

59. TMEP, *supra* note 36, § 904.03. All marks will eventually include a specimen, but specimens are only required for applications filed on an in-use basis. *Id.* Searching for trademark applications that include a specimen requires a Structured Search in TESS, in which the Search Term is “1A” and the Field is “Current Basis.”

the application.”⁶⁰ According to the Trademark Trial and Appeals Board, “[a]n important function of specimens in a trademark application is, manifestly, to enable the PTO to verify the statements made in the application regarding trademark use.”⁶¹ Effectively, specimens serve as visual demonstrations that the mark for which registration is sought is used in connection with at least one good (or service) in each class of goods or services identified in the application for registration.⁶²

The type of specimen varies based on the goods or services on which the mark is used. Specimens for hardware, for example, may take the form of commercial packaging.⁶³ Specimens for software, however, are likely to take the form of a screenshot of the software interface or a website offering the software for sale.⁶⁴ Although the contents of specimens are not searchable using TESS, specimens for in-use applications or registered trademarks can reveal details about surveillance technologies, from the physical configuration of surveillance hardware,⁶⁵ to the features of surveillance software,⁶⁶ to the location of law enforcement customers.⁶⁷

III. REVEALING DISCLOSURES IN TRADEMARK FILINGS FOR SURVEILLANCE TECHNOLOGIES

Revealing a surveillance technology using federal trademark filings opens new avenues for journalists, researchers, and civil society to leverage those disclosures. One may discover that a surveillance technology is in development

60. TMEP, *supra* note 36, § 904.

61. Application of Bose Corp., 546 F.2d 897 (C.C.P.A. 1976). The Federal Circuit made similar observations. *See In re Sones*, 590 F.3d 1282, 1284 (Fed. Cir. 2009) (observing that the USPTO requires specimens to ensure that applicants are using the mark in commerce).

62. TMEP, *supra* note 36, § 904.01. The TMEP offers extensive guidance about the forms that certain specimens may take. *See* TMEP, *supra* note 36, § 904. An effort to reform the process for federal trademark registration to require fewer disclosures would likely target specimens. However, specimens are a crucial piece of the registration process that ought to go unchanged, despite possible future challenges from industry.

63. TMEP, *supra* note 36, § 904.03(e).

64. *Id.*; *In re Azteca Sys., Inc.*, 102 U.S.P.Q.2d 1955 (T.T.A.B. 2012). Screenshots of websites merely advertising the software are insufficient as specimens. TMEP, *supra* note 36, § 904.03(e). Similarly, displays associated with goods, including advertising and promotional materials, are not “per se ‘displays’” that qualify as sufficient specimens. *See id.* § 904.03(g).

65. *See infra* Part III.A.

66. *See infra* Parts III.B–C.

67. *See, e.g.*, SHOTSPOTTER, Registration No. 3896150, Specimen (Feb. 25, 2016) (featuring a map identifying more than 50 cities across the United States, Brazil, Panama, and the United Kingdom using ShotSpotter technology, along with the years those cities began using the technology).

before there has been a public announcement.⁶⁸ One may uncover a surveillance technology whose existence has been obfuscated by non-disclosure agreements between a company and law enforcement.⁶⁹ One may find that the maker of a surveillance technology potentially exposed personal information about a target publicly.⁷⁰ Or one may unearth the terms of the financial arrangement between a company and law enforcement.⁷¹ Each revelation presents a new opportunity to bring new information about surveillance technologies to light so that the public may play a role in deciding how these technologies are deployed—or whether they’re deployed at all.

These examples form the basis of three original case studies of Harris Corporation’s STINGRAY mark, Vigilant Solution’s VIGILANT SOLUTIONS mark, and PredPol’s PREDPOL mark. This Part explores these case studies using real trademark filings to illustrate how applications for registration of trademarks can be a source of transparency about surveillance technology, even when other transparency mechanisms fall short.

A. STINGRAY: CELL-SITE LOCATION INFORMATION INTERCEPTORS

Modern mobile phones disclose a significant amount of sensitive personal information, such as who we call, how long we talk to them, and our real-time locations. With that wealth of information at the ready, it is not surprising that law enforcement has an interest in capturing these details at the source.⁷² Enter cell-site location information interceptors, or CSLI interceptors.⁷³ CSLI interceptors mimic cell phone communications towers in such a way that all nearby cell phones, including those of innocent passersby, are “tricked” into communicating with an interceptor rather than a cell tower operated by a telecommunications provider.⁷⁴

68. See, e.g., *supra* Part I.

69. See *infra* Part III.A.

70. See *infra* Part III.B.

71. See *infra* Part III.C.

72. Larry Greenemeier, *What Is the Big Secret Surrounding Stingray Surveillance*, SCI. AM. (June 25, 2015), <https://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/>.

73. For a discussion of the detailed information that can be revealed by CSLI, see *Carpenter v. United States*, 138 S. Ct. 2206, 2211–13 (2018). These devices are also sometimes referred to as international mobile subscriber identity, or IMSI, catchers.

74. Ryan Gallagher, *Meet the Machines That Steal Your Phone’s Data*, ARS TECHNICA (Sept. 25, 2013), <https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/>.

Harris Corporation, a defense contractor based in Melbourne, Florida,⁷⁵ makes one of the most popular CSLI interceptors, sold under the brand name STINGRAY.⁷⁶ The Stingray device has become so popular in the market that “stingray” often generically refers to the whole class of technologies known as cell-site simulators.⁷⁷ Since introducing the Stingray device, Harris Corporation has taken steps to avoid transparency about its surveillance technology: Harris Corporation’s website omitted any information about Stingray devices, and marketing materials came with warnings that distribution outside law enforcement or telecommunications firms could be a crime, punishable by up to five years in prison.⁷⁸ Harris Corporation petitioned the Federal Communications Commission to prevent disclosure of Stingray user manuals in response to public records requests.⁷⁹ The company even went so far as to demand that law enforcement using Stingray devices agree and adhere to strict

75. *Locations*, HARRIS CORP., <https://www.harris.com/locations> (last visited Mar. 20, 2018) (noting the location of their corporate headquarters).

76. STINGRAY, Registration No. 2762468 (Sept. 9, 2003). Harris Corporation makes many other pieces of surveillance technology, including DENALI, Registration No. 5628200 (filed Dec. 11, 2018) (Class 9 covering, in part, “firmware installable in communications transceivers for enabling such transceivers to encrypt and decrypt information communicated via the transceivers”), and KINGFISH, Registration No. 2867227 (July 27, 2004) (Class 9 covering “electronic surveillance transceivers for tracking, locating and gathering information from cellular telephones”).

77. *See, e.g.*, Jennifer Valentino-DeVries, “*Stingray*” Phone Tracker Fuels Constitutional Clash, WALL ST. J. (Sept. 22, 2011), <https://www.wsj.com/articles/SB10001424053111904194604576583112723197574>; Gallagher, *supra* note 74 (noting that the term “stingray” is used generically). The terms “cell site location information interceptors” and “cell-site simulators” are used interchangeably.

78. Gallagher, *supra* note 74.

79. Letter from Tania W. Hanna, Vice President of Government Relations, Harris Corp., to Julius P. Knapp, Chief of Office of Engineering and Technology, FCC, Request for Confidentiality of Harris Corporation for FCC ID Nos. NK73092523, NK73100176, NK73166210 (Oct. 20, 2014), <https://www.scribd.com/document/259988405/Harris-Letter-Response-Request-for-Confidentiality-FOIA-2014-669>; Matthew Keys, *Exclusive: StingRay Maker Asked FCC To Block Release of Spy Gear Manual*, THE BLOT (Mar. 26, 2015), <https://www.theblot.com/exclusive-stingray-maker-asked-fcc-to-block-release-of-spy-gear-manual-7739514>; *see also* Nathan Freed Wessler & Nicole Ozer, *Documents Suggest Maker of Controversial Surveillance Tool Misled the FCC*, ACLU: FREE FUTURE (Sept. 17, 2014), <https://www.aclu.org/blog/documents-suggest-maker-controversial-surveillance-tool-misled-fcc?redirect=blog/national-security/documents-suggest-maker-controversial-surveillance-tool-misled-fcc> (observing that Harris claimed that its Stingray technology would only be used for emergencies despite records released by the Tallahassee, Florida Police Department suggesting that only 29% of cases involving a Stingray were “emergencies”).

non-disclosure agreements prohibiting those agencies from disclosing any details about Harris' equipment, including its existence—even to judges.⁸⁰

Perhaps Harris Corporation's dedication to avoiding transparency explains why it took some time for the public to receive its first federal case to mention Stingray devices.⁸¹ In *United States v. Allums*, the defendant, James Edward Allums, was charged with three robberies, in part based on the CSLI of Allums' cell phone.⁸² As Judge Stewart explained, the government used a phone and "another device called a Stingray, which also tracked which cell tower was the strongest at any geographical position," to identify the location of Allums.⁸³ The unpublished memorandum decision was released in 2009, but it took until 2014 for the American Civil Liberties Union to use a public records request to obtain emails (also written in 2009) revealing that law enforcement in Florida had been misleading judges, defense counsel, and defendants about the use of Stingray devices.⁸⁴

80. *See, e.g.*, *Thomas v. State*, 127 So.3d 658, 660 (Fla. Dist. Ct. App. 2013) (noting that local police department "did not want to obtain a search warrant because they did not want to reveal information about the technology they used to track the cell phone signal" due to a non-disclosure agreement with Harris Corporation); *see also* Kim Zetter, *Police Contract with Spy Tool Maker Prohibits Talking About Device's Use*, WIRED (Mar. 4, 2014), <https://www.wired.com/2014/03/harris-stingray-nda/> (providing an example of an NDA attached to the use of police surveillance equipment); Spencer McCandless, Note, *Stingray Confidential*, 85 GEO. WASH. L. REV. 993 (2017), <http://www.gwlr.org/wp-content/uploads/2017/07/85-Geo.-Wash.-L.-Rev.-993.pdf> (considering the long history of the use of "stingray" devices and the secrecy surrounding them).

81. *United States v. Allums*, No. 2:08-CR-30 TS (D. Utah, Mar. 24, 2009). The *Rigmaiden* case, which involved a pro se defendant who successfully demonstrated that a warrantless cell-site location information interceptor was used to investigate his case, is often identified as the first case to publicly reveal the existence of Stingray devices—but the final decision, which discussed Stingray devices, was not decided until 2013. *See United States v. Rigmaiden*, No. CR 08-814-PHX-DGC (D. Ariz. May. 8, 2013). That said, similar devices were in use well before 2009—the Harris Corporation's Triggerfish device was promoted as early as 1991. *See* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 142 (2014) ; *see also* Tsutomu Shimomura, *Catching Kevin*, WIRED (Feb. 1, 1996), <https://www.wired.com/1996/02/catching/> (describing how a cell-site simulator was used to track hacker Kevin Mitnick, along with a Triggerfish device). The earliest trademark application for the TRIGGERFISH mark was filed in 2001. *See* TRIGGERFISH, Registration No. 2534253 (Jan. 29, 2002)(cancelled Oct. 31, 2008).

82. *Allums*, No. 2:08-CR-30 TS at 1.

83. *Id.* at 2.

84. Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, ACLU: FREE FUTURE (June 19, 2014), <https://www.aclu.org/blog/national-security/privacy-and-surveillance/internal-police-emails-show-efforts-hide-use-cell?redirect=blog/national-security-technology-and-liberty/internal-police-emails-show-efforts-hide-use-cell>.

If someone had been scanning federal trademark filings, however, the public would have known about the existence of Stingray devices nearly a decade sooner.⁸⁵ On August 21, 2001, Harris Corporation filed a federal trademark application for the STINGRAY mark.⁸⁶ The mark was filed with an intent-to-use designation, with the first use date of March 2, 2003.⁸⁷ As registered, the mark covers “multi-channel, software-defined, two-way electronic surveillance radios for authorized law enforcement agencies for interrogating, locating, tracking and gathering information from cellular telephones” in Class 9.⁸⁸ The specimen depicts an actual Stingray device, emblazed with the logo, and depicting the inputs and outputs embedded in the device.⁸⁹

Using federal trademark filings, the public could have learned about the existence of CSLI interceptors nearly a decade before the first federal court decision disclosing the existence of Stingray devices.

85. Harris Corporation also patented the Stingray device even earlier than filing its trademark application. U.S. Patent No. 5428667A (June 27, 1995), <https://patents.google.com/patent/US5428667A/en>.

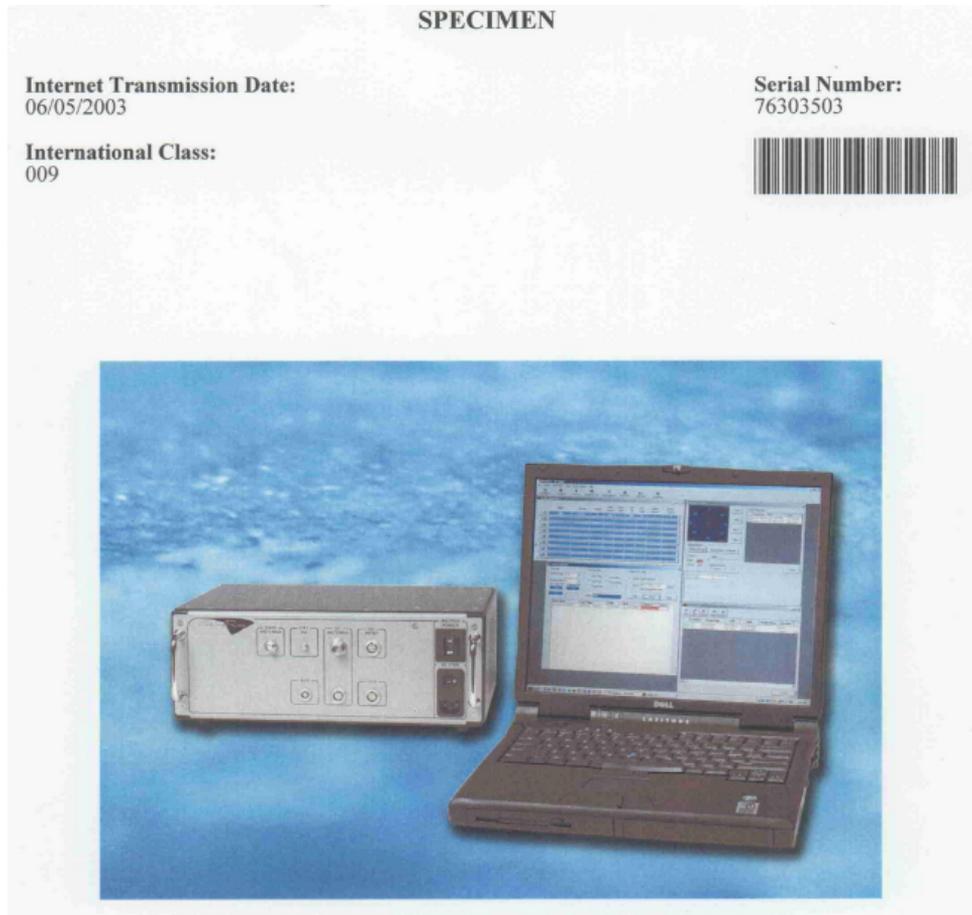
86. STINGRAY, Registration No. 2762468 (Sept. 9, 2003).

87. *Id.*

88. *Id.*

89. STINGRAY, Registration No. 2762468, Specimen (June 18, 2003). The specimen was the second specimen submitted; the prior specimen borders on illegible due to the quality of the images included. *See* STINGRAY, Registration No. 2762468 (June 5, 2003).

Figure 1: Stingray CSLI Interceptor



B. VIGILANT SOLUTIONS: AUTOMATED LICENSE PLATE READERS

Certain private corporations regularly take photographs of cars, trucks, and other automobiles and sell those images to law enforcement. These companies mount small high-speed cameras called automated license plate readers, or ALPRs, on moving police vehicles or stationary infrastructure like bridges or

roads,⁹⁰ which then photograph up to thousands of license plates per minute.⁹¹ The photographs are then stored in searchable databases used by law enforcement.⁹² According to the International Association of Chiefs of Police, law enforcement agencies can use ALPRs to “enhance their enforcement and investigative capabilities, expand their collection of relevant data, and expedite the tedious and time consuming [sic] process of comparing vehicle license plates with lists of stolen, wanted, and other vehicles of interest.”⁹³ ALPRs also enable surveillance by empowering law enforcement to track a single vehicle across cities and states with no suspicion of wrongdoing—a task that would be challenging, if not impossible, for someone peeking out of a window and jotting down license plate numbers.⁹⁴

ALPR databases are also abused blatantly.⁹⁵ In 2016, for example, a Washington D.C. police officer pleaded guilty to extortion after blackmailing car owners whose vehicles were identified near a gay bar.⁹⁶ The year before, a SWAT team mistakenly raided a man’s house searching for a marijuana-growing operation because of license plate monitoring at a garden store but found no evidence of such an operation.⁹⁷ And several years before that, police

90. Ellen Nakashima & Josh Hicks, *Homeland Security is Seeking a National License Plate Tracking System*, WASH. POST (Feb. 18, 2014), https://www.washingtonpost.com/world/national-security/homeland-security-is-seeking-a-national-license-plate-tracking-system/2014/02/18/56474ae8-9816-11e3-9616-d367fa6ea99b_story.html?noredirect=on&utm_term=.876d14309e14.

91. *Automatic License Plate Readers*, AM. CIV. LIBERTIES UNION, <https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers> (last visited Mar. 20, 2018).

92. See generally *Vigilant Platesearch*TM, VIGILANT SOLUTIONS, <https://www.vigilant-solutions.com/products/license-plate-recognition-lpr/> (last visited Feb. 22, 2020).

93. *Automated License Plate Recognition*, INT’L ASS’N OF CHIEFS OF POLICE, <https://www.theiacp.org/projects/automated-license-plate-recognition> (last visited Mar. 20, 2018).

94. For a comprehensive exploration of local law enforcement use of ALPRs and the transparency challenges posed by those relationships, see generally Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 MAINE L. REV. 398 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341182.

95. Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, WALL ST. J. (Sept. 29, 2012), <https://www.wsj.com/articles/SB10000872396390443995604578004723603576296>.

96. Anthony D. Romero, *Documents Uncover NYPD’s Vast License Plate Reader Database*, HUFFINGTON POST (Jan. 26, 2016), https://www.huffingtonpost.com/mariko-hirose-/documents-uncover-nypds-v_b_9070270.html; see also Mariko Hirose, *Documents Uncover NYPD’s Vast License Plate Reader Database*, ACLU: FREE FUTURE (Jan. 25, 2016), <https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database>.

97. Radley Balko, *Federal Judge: Drinking Tea, Shopping at a Gardening Store is Probable Cause for a SWAT Raid on Your Home*, WASH. POST (Dec. 28, 2015), <https://>

removed a woman from her car at gunpoint on the mistaken belief that she was driving a stolen car after a license plate reader had misread her plates.⁹⁸

Most states do not regulate ALPRs.⁹⁹ But sixteen states, including California, Florida, and Maryland, do have laws regarding license plate readers and data retention.¹⁰⁰ These laws can still be insufficient to deter misconduct. In early 2020, a California auditor discovered widespread issues with use of license plate readers across in the state, from insecurely storing data to sharing images with thousands of entities across the United States without determining whether those entities had a right or need to access the images.¹⁰¹

One of the leading ALPR vendors is Vigilant Solutions, a company based in Livermore, California.¹⁰² Vigilant Solutions takes information that can be unwieldy to manage and collect—like photographs of license plates—and assembles that information into databases for private clients.¹⁰³ In its marketing materials, Vigilant Solutions advertises that its license plate recognition tools scan photographs of license plates along with the date, time, and location of where a particular vehicle was photographed.¹⁰⁴ Chris Metaxas, a chief

www.washingtonpost.com/news/the-watch/wp/2015/12/28/federal-judge-drinking-tea-shopping-at-a-gardening-store-is-probable-cause-for-a-swat-raid-on-your-home/?utm_term=.44d1bc082ee9; Romero, *supra* note 96.

98. Kade Crockford, *San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error*, ACLU: FREE FUTURE (May 13, 2014), <https://www.aclu.org/blog/privacy-technology/location-tracking/san-francisco-woman-pulled-out-car-gunpoint-because>.

99. *Automated License Plate Readers: State Statutes*, NAT'L CONF. OF STATE LEGISLATURES, <http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx> (updated Oct. 23, 2020).

100. *Id.* Arkansas, Colorado, Georgia, Maine, Minnesota, Montana, Nebraska, New Hampshire, North Carolina, Oklahoma, Tennessee, and Utah also have ALPR laws. *Id.* Vermont repealed its ALPR law in 2020. See *Vermont Statutes Online*, VT. GEN. ASSEMBLY, <https://legislature.vermont.gov/statutes/section/23/015/01607> (last visited Nov. 19, 2020).

101. ELAINE M. HOWLE, CALIFORNIA STATE AUDITOR, REPORT NO. 2019-118: SUMMARY OF AUTOMATED LICENSE PLATE READERS: TO BETTER PROTECT INDIVIDUALS' PRIVACY, LAW ENFORCEMENT MUST INCREASE ITS SAFEGUARDS FOR THE DATA IT COLLECTS (2020), <https://www.auditor.ca.gov/reports/2019-118/index.html>.

102. *Our Passion*, VIGILANT SOLUTIONS, <https://www.vigilantsolutions.com/our-passion/> (last visited Nov. 17, 2020). Based on its website, Vigilant Solutions is expanding into facial recognition technology. See *Vigilant Facesearch*TM, VIGILANT SOLUTIONS, <https://www.vigilantsolutions.com/products/facial-recognition/> (last visited Oct. 28, 2019).

103. Dan Froomkin, *Reports of the Death of a National License-Plate Tracking Database Have Been Greatly Exaggerated*, THE INTERCEPT (Mar. 17, 2014), <https://theintercept.com/2014/03/17/1756license-plate-tracking-database/> (detailing the national network of license plate databases).

104. *Vigilant Solutions, PlateSearch*, VIGILANT SOLUTIONS, https://www.motorola.com/content/dam/msi/docs/products/license-plate-recognition-systems/reaperhd-mobile-lpr-system/vigilant_platesearch_fact_sheet.pdf (last visited Aug. 8, 2021).

executive for Vigilant Solutions' subsidiary DRN, compared the company's work to "a guy holding his head out the window, looking down the block, and writing license-plate numbers down and comparing them against a list. The technology just makes things better and more productive."¹⁰⁵ Vigilant Solutions' technology certainly makes surveillance easier: Vigilant Solutions advertises that its commercial dataset offers more than 5 billion license plate detections, with more than 150 million plates added each month.¹⁰⁶

Discovering information about ALPRs can be challenging. In 2018, the Electronic Frontier Foundation (EFF) used public records requests to find out more information about the procurement and deployment of ALPRs. EFF partnered with Muckrock—a nonprofit organization dedicated to public records requests—to file a series of requests to gather details about more than 200 cities' ALPR programs.¹⁰⁷ Responses to these requests revealed that fewer than 1% of the 2.5 billion license plates scanned in the years 2016 and 2017 were linked to cars under any suspicion at the time the plates were captured.¹⁰⁸ EFF concluded that law enforcement agencies shared their data with a minimum of 160 other agencies, all through Vigilant Solutions' LEARN program, an acronym for Law Enforcement Archival and Reporting Network.¹⁰⁹ In response to EFF and MuckRock's FOIA requests, Vigilant Solutions reached out to at least one jurisdiction to assure the city that "quite simply...we are here for you."¹¹⁰

105. Nakashima & Hicks, *supra* note 90.

106. *Vigilant Solutions*, MOBILCOMM (last visited Nov. 18, 2020), <https://www.mobilcomm.com/vigilant-solutions/>; see also Gwyndolyn Wu, *ICE Had Access to Hundreds of Millions of License Plates*, S.F. CHRON. (Mar. 13, 2019), <https://www.sfchronicle.com/crime/article/ICE-had-access-to-hundreds-of-millions-of-license-13685652.php>.

107. David Maass & Beryl Lipton, *EFF and MuckRock Release Records and Data from 200 Law Enforcement Agencies' Automated License Plate Reader Programs*, EFF DEEPLINKS (Nov. 15, 2018), <https://www.eff.org/deeplinks/2018/11/eff-and-muckrock-release-records-and-data-200-law-enforcement-agencies-automated>; see also Cory Doctorow, *Here's the Secret Details of 200 Cities' License-Plate Tracking Programs*, BOINGBOING (Nov. 15, 2018), <https://boingboing.net/2018/11/15/find-yourself-a-city-to-live-i.html>.

108. Dave Maass & Beryl Lipton, *Data Driven: Explore How Cops Are Collecting and Sharing Our Travel Patterns Using Automated License Plate Readers*, EFF, <https://www.eff.org/pages/automated-license-plate-reader-dataset> (last visited Nov. 19, 2020).

109. *Id.* Vigilant Solutions has been unimpressed by EFF's investigations into its technology and policies. See, e.g., Susan Crandall, *EFF: Stop Creating Fake News and Scaring People!*, VIGILANT SOLUTIONS (July 12, 2018), <https://www.vigilantsolutions.com/eff-stop-creating-fake-news-scaring-people/> (responding to an EFF investigation that linked a Vigilant Solutions customer that manages several California malls to vehicle data shared with Immigration and Customs Enforcement (ICE)).

110. Camille Fassett, *License Plate Surveillance Company Attacks Nonprofits for Filing FOIA Requests*, VICE (Apr. 4, 2018), <https://www.vice.com/en/article/3kjp85/vigilant-solutions-eff-muckrock-foia-requests>.

Vigilant Solutions has two federally registered trademarks. One is a design mark for a three-part disjointed V with the words VIGILANT SOLUTIONS stacked on top of one another to the right of the V, was filed on June 26, 2014.¹¹¹ The VIGILANT SOLUTIONS design mark covers “computer hardware and software in the fields of law enforcement and crime prevention for identifying human faces and vehicle license plates, for tracking vehicles over time and geographic location, and for producing reports on the movements of specific vehicles” in Class 9.¹¹²

But it is the VIGILANT SOLUTIONS specimen that is especially revealing—it features what appears to be authentic geolocation data linked to real license plate numbers:

Figure 2: Vigilant Solutions LEARN Interface

Applicant: Vigilant Solutions, Inc.

Mark: VIGILANT SOLUTIONS & V Design

The screenshot displays the LEARN (Law Enforcement Archival & Reporting Network) interface. At the top left is the Vigilant Solutions logo. The main header reads "LEARN Law Enforcement Archival & Reporting Network" with navigation links for Back, Home, and Log Out. A "Search Plate" section is visible on the left. The central area shows a "Detection Details" popup over a satellite map. The popup contains the following information:

| Detection Date | |
|-----------------------|------------------------|
| Vehicle Info: | Camera Info: |
| Plate #1: XE28693 | Agency: N/A |
| Plate #2: A883HB | User: Private Data |
| Date: 05-08-13 | System: Private System |
| Time: 8:50:33 AM | Camera: N/A |
| Longitude: -78.282889 | Type: N/A |
| Latitude: 36.784207 | |

Additional details in the popup include:

- Nearest Address: Dan Neck Road, Virginia Beach, VA 23463
- Nearest Intersection: Dan Neck Rd, London Bridge Rd
- Disclaimer: The address listed above is ONLY an address.

Below the popup, a table of search results is shown with columns: Image, Plate, Date, Time, Scanned By, and System. The table contains several entries, including:

| Image | Plate | Date | Time | Scanned By | System |
|-------|---------|----------|------------------|--------------|-------------|
| | ABX255 | 05-08-13 | 7:50:35 AM EST | Private Data | Private Sys |
| | YG58780 | 05-08-13 | 8:50:33 AM -0400 | Private Data | Private Sys |
| | XE28693 | 05-08-13 | 8:50:33 AM -0400 | Private Data | Private Sys |
| | A883HB | 05-08-13 | 8:50:32 AM CST | Private Data | Private Sys |
| | A883HB | 05-08-13 | 8:50:32 AM CST | Private Data | Private Sys |

At the bottom of the interface, there are buttons for "Output Report", "Customize View", and "Save Search". A footer note reads "LEARN V.5.0 2012 Copyright Vigilant Solutions All Rights Reserved" and "Protecting Officers, Families and Communities".

111. VIGILANT SOLUTIONS, Registration No. 4780381 (July 28, 2015).

112. *Id.*

Vigilant Solutions appears to have submitted an image from its LEARN database depicting four license plate numbers, all of which are clearly legible in the specimen.¹¹³ The specimen also appears to reveal the precise latitude and longitude data for a specific license plate number.¹¹⁴ According to the specimen, the plate was identified through private data and a private system on Dam Neck Road in Virginia Beach, Virginia.¹¹⁵ The specimen includes a visualization of the location.¹¹⁶

The other, earlier registration is for the image of a disjointed V, filed on August 13, 2013.¹¹⁷ The mark covers “[c]omputer hardware and software in the fields of security and law enforcement for tracking vehicles over time and geographic location and for producing reports on the movements of specific vehicles” in Class 9.¹¹⁸

The specimen appears to show an interface for a “Vigilant Stakeout—Report” and depicts an exact address in Homestead, Florida.¹¹⁹ Visit number 21 is highlighted with 531 plates scanned, but the target plate does not appear to have been scanned.¹²⁰ The bottom of the specimen features five images of car bumpers, each featuring their respective license plate numbers, as well as the date and time the cars were scanned.¹²¹

113. VIGILANT SOLUTIONS, Registration No. 4780381, Specimen (June 26, 2014).

114. *Id.*

115. *Id.*

116. *Id.*

117. VIGILANT SOLUTIONS, Registration No. 4528520 (May 13, 2014).

118. *Id.*

119. VIGILANT SOLUTIONS, Registration No. 4528520, Specimen (Aug. 13, 2013).

120. *Id.*

121. *Id.*

Figure 3: Vigilant Solutions LEARN Interface

Applicant: Vigilant Solutions, Inc.

Mark: VIGILANT SOLUTIONS & V Design

The screenshot displays the LEARN (Law Enforcement Archival & Reporting Network) interface. At the top, the Vigilant Solutions logo is on the left, and the title 'LEARN Law Enforcement Archival & Reporting Network' is on the right. Below the title are navigation links for 'Back', 'Home', and 'Log Out'. The main area is divided into several sections:

- Search Plate:** A search bar with a 'Search' button.
- Detection Details:** A pop-up window showing a map with a red circle indicating a location. To the right of the map is a table of detection details:

| Detection Data | | Camera Info: | |
|---|------------|--------------|----------------|
| Vehicle Info: | | Agency: | N/A |
| Plate # 1: | XE28693 | User: | Private Data |
| Plate # 2: | AF28693 | System: | Private System |
| Date: | 05-08-13 | Camera: | N/A |
| Time: | 8:50:33 AM | Type: | N/A |
| Longitude: | -76.520289 | | |
| Latitude: | 36.794597 | | |
| Nearest Address: Cap Neck Road, Virginia Beach, VA, 23463 | | | |
| Nearest Intersection: Cap Neck Rd, London Bridge Rd | | | |
| Disclaimer: The address listed above is ONLY an estimate. | | | |
- Associate Analysis:** A section with a 'Go to Page' dropdown (set to 1) and a 'Records Per Page' dropdown (set to 50).
- Table of Results:** A table with columns: Image, Plate, Date, Time, Scanned By, and System. It shows several rows of vehicle detections, including one with plate XE28693 and another with plate A883HB.
- Buttons:** 'Output Report', 'Customize View', and 'Save Search' are located below the table.
- Footer:** 'LEARN V.5.0 2012 Copyright Vigilant Solutions All Rights Reserved' and 'Protecting Officers, Families and Communities'.

Vigilant Solutions' trademark filings offer an additional approach to surveillance transparency, in which the public reveals that a company may have failed to protect the sensitive information that it collects.¹²² There has already been backlash to the deployment of ALPRs in communities without public approval,¹²³ and these specimens may further fuel transparency by offering journalists and civil liberties organizations an alarming new talking point.

C. PREDPOL: PREDICTIVE POLICING ALGORITHMS

Predictive policing uses algorithms that attempt to predict the geographical locations of future crimes using data drawn from past crime statistics and other

122. See *supra* note 119.

123. It's worth noting that some reports suggest that surveillance cameras, like those that fuel ALPR systems, do not have a measurable impact on reducing crime. See, e.g., Sonia Roubini, *Police Chief: Surveillance Cameras Don't Help Fight Crime*, ACLU: FREE FUTURE (Apr. 9, 2015), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-chief-surveillance-cameras-dont-help-fight>.

information.¹²⁴ The company PredPol describes itself as the market leader in predictive policing technology.¹²⁵ The “past crime statistics and other information” used by PredPol’s algorithm include victimization data, meaning crimes that have been reported to law enforcement.¹²⁶

PredPol is not without controversy. Relying on crime data that reflects systemic racial bias as training data—dubbed “dirty data” by Rashida Richardson, Kate Crawford, and Jason Schultz—can effectively amplify those biases.¹²⁷ PredPol remains a private company, developed from research conducted by the University of California, Los Angeles and the Los Angeles Police Department,¹²⁸ but only individuals who have financial interests in PredPol have conducted research on the company’s methodology.¹²⁹ Some of those jurisdictions, like the Los Angeles Police Department, have been candid and forthcoming about their use of PredPol algorithms to evaluate crimes.¹³⁰

Others have been far less transparent, leading researchers to resort to clever techniques to try to learn more about PredPol’s partnerships and practices. In 2018, a security researcher used a series of domain-name logins to identify a dozen cities with previously undisclosed relationships with PredPol.¹³¹ Journalist Caroline Haskins used the domain names as a starting

124. Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259 (2012). For a comprehensive accounting of attempts to bring oversight to predictive policing technologies, see generally FERGUSON, *THE RISE OF BIG DATA POLICING* (2017) and Andrew G. Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109 (2017) (hereinafter *Policing Predictive Policing*).

125. *Overview*, PREDPOL, <https://www.predpol.com/about/> (last visited Mar. 18, 2019).

126. *Id.* As Ferguson notes, “PredPol’s primary business of targeting burglary and auto-related crimes avoids many of the data collection problems of a broader crime focus.” *Policing Predictive Policing*, *supra* note 124, at 1148.

127. Rashida Richardson, Kate Crawford & Jason Schultz, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, N.Y.U. L. REV. ONLINE (forthcoming). For a discussion of implicit bias becoming embedded in artificial intelligence systems, see generally Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence’s Implicit Bias Problem*, 93 WASH. L. REV. 579 (2018).

128. PREDPOL, *supra* note 125; see also Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J. L. & TECH. 103, 146 (2018).

129. Emily Berman, *A Government of Laws and Not of Machines*, 98 BOSTON U. L. REV. 1277, 1307 (2018) (citing Darwin Bond Graham, *Oakland Mayor Schaaf and Police Seek Unproven “Predictive Policing” Software*, EAST BAY EXPRESS (June 24, 2015), <https://www.eastbayexpress.com/oakland/oakland-mayor-schaaf-and-police-seek-unproven-predictive-policing-software/Content?oid=4362343>).

130. See Ferguson, *supra* note 124, at 261; see also Leila Miller, *LAPD Will End Controversial Program that Predicts Where Crimes Would Occur*, L.A. TIMES (Apr. 21, 2020), <https://www.latimes.com/california/story/2020-04-21/lapd-ends-predictive-policing-program>.

131. Cory Doctorow, *Is This the Full List of US Cities That Have Bought Or Considered PredPol’s Predictive Policing Services?*, BOINGBOING (Oct. 30, 2018), <https://boingboing.net/2018/10/30/el-monte-and-tacoma.html>.

point for her own series of public record requests for PredPol contracts and negotiation emails, instruction manuals, and slide presentations.¹³² That same year, researchers Ellen Goodman and Robert Brauneis sent public records requests to eleven police departments, eight of which declined to respond or acknowledged the request without producing any responsive documents.¹³³ One city even stated that “[t]he City Attorney has advised that information revealing surveillance techniques, procedures or personnel is exempt from public inspection pursuant to s. 119.071(2)(d), Florida statutes.”¹³⁴

Neither investigation revealed a relationship between PredPol and the city of Richmond, California, a small city in the East Bay.¹³⁵ The existence of Richmond’s contract with PredPol was not exactly a secret,¹³⁶ but the details were revealed somewhere surprising: federal trademark filings.¹³⁷ PredPol filed a trademark application for the PREDPOL mark on February 2, 2012 covering, in part, “computer software for use in law enforcement and related business, namely, computer software used for use in the analysis and determination of probable locations where crimes will be committed with information delivery through browser and portable device applications and map overlays” in Class 9.¹³⁸

132. Caroline Haskins, *Dozens of Cities Have Secretly Experimented with Predictive Policing Software*, MOTHERBOARD, Feb. 6, 2019, <https://www.vice.com/en/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software>.

133. Brauneis & Goodman, *supra* note 128, at 146–47.

134. *Id.* at 147 (quoting Legislation Details (With Text), CITY OF COCOA, FILE # 15-361, (July 30, 2015), http://cdn.muckrock.com/foia_files/2017/01/13/15-361_City_Council_Agenda_Item__8-25-15.pdf).

135. *Richmond, California*, WIKIPEDIA, https://en.wikipedia.org/wiki/Richmond,_California (last visited Mar. 18, 2018).

136. *SF Weekly* reported that Richmond was using PredPol technology in 2013. Darwin Bond-Graham, *All Tomorrow’s Crimes: The Future of Policing Looks a Lot Like Good Branding*, SF WEEKLY (Oct. 30, 2013), <http://www.sfweekly.com/news/all-tomorrows-crimes-the-future-of-policing-looks-a-lot-like-good-branding/>. The *East Bay Express* published a critical follow up several years later. See Bond-Graham, *supra* note 129. Unlike some acquisitions of surveillance technologies, Oakland Mayor Libby Schaaf disclosed the contract with PredPol in her 2015-2017 budget for the city. *Id.*

137. PREDPOL, Registration No. 4299222 (Mar. 5, 2013).

138. *Id.*

Figure 4: PredPol Contract



PREDICTIVE POLICING

THE PREDICTIVE POLICING COMPANY

PROPOSED TERMS for PREDICTIVE POLICING DEPLOYMENT

August 2, 2012

PredPol is glad to be working with you on decreasing the City's crime and looks forward to a very productive and successful relationship. These are proposed terms of the Richmond, CA ("City"), deployment of PredPol:

1. Financial Parameters:
 - a. List price for a municipality the size of Columbia is \$75,000.
 - b. Setup fee for a municipality the size of Columbia is \$15,000.
 - c. Columbia will receive a 33% discount on the annual subscription fee for PredPol, to \$50,000 per year.
 - d. Setup fee will be waived.
 - e. Term of the subscription will be three years.
 - f. Additional discounts in subsequent years based on deployment of the tool across other, adjacent jurisdictions are available.
2. Non-Financial Parameters: In consideration of the discounted pricing provided by PredPol, City agrees to *reasonably* support PredPol's research and development by doing the following, during the term of this Agreement:
 - a. Deploy and utilize the PredPol tool and the intelligence it generates;
 - b. Generally support the testing of the PredPol tool and any new features/tools, including providing user feedback, as requested by PredPol;
 - c. Provide access to relevant City databases and shared databases to which the City has access, pursuant to all applicable laws and access agreements;
 - d. Contribute to requested case studies on predictive policing;
 - e. Provide public testimonials and referrals to other agencies;
 - f. Respond to inquiries and host visitors from other agencies;
 - g. Engage in reasonable joint/integrated marketing, including but not limited to press conferences and media relations, training materials, marketing, tradeshows, conferences, speaking engagements and research. In the event any of the forgoing would involve costs to the City outside of their normal costs for employees performing their normal job duties, PredPol agrees to reimburse City for such costs. For example, if a Chief is requested to attend and speak at a conference of Police Chiefs to which they are not already traveling, PredPol agrees to reimburse City for travel expenses, if requested.

CONTACT:

1 | CONFIDENTIAL

PREDICT CRIME IN REAL TIME™

On December 13, 2012, PredPol submitted a specimen showing the PREDPOL mark as used in commerce.¹³⁹ The majority of the specimen appears to be marketing materials explaining the mechanics of how PredPol

139. PREDPOL, Registration No. 4299222, Specimen (Dec. 13, 2012). The specimen has been lightly redacted, as the original specimen uploaded by PredPol reveals the cell phone number of someone who appears to be an employee.

works and the ways in which it can benefit law enforcement.¹⁴⁰ But, beginning on the third page, PredPol submitted a contract that lays out the proposed terms for a PREDPOL software deployment for the city of “Richmond, CA.”¹⁴¹ The contract begins by explaining that “PredPol is glad to be working with you on decreasing the City’s crime and looks forward to a very productive and successful relationship.”¹⁴²

The contract is dated August 2, 2012,¹⁴³ and it identifies the financial parameters for the agreement. It states that the “list price for a municipality the size of Columbia is \$75,000” and the “setup fee is...\$15,000.”¹⁴⁴ The contract appears to provide Richmond with two discounts: “Columbia [*size*] will receive a 33% discount on the annual subscription fee for PredPol, to \$50,000 per year” and the “[s]etup fee will be waived.”¹⁴⁵ The term of the subscription is three years.¹⁴⁶ There is also a provision providing that “[a]dditional discounts in subsequent years based on deployment of the tool across other, adjacent jurisdictions are available.”¹⁴⁷

The most shocking term of the contract is Richmond’s agreement to support PredPol and its work in exchange for the discounted pricing.¹⁴⁸ The contract states that “City agrees to *reasonably* support PredPol’s research and development by doing the following, during the term of this Agreement...[p]rovide public testimonials and referrals to other agencies” and “[e]ngage in reasonable joint/integrated marketing, including but not limited to press conferences and media relations, training materials, marketing, tradeshows, conferences, speaking engagements and research.”¹⁴⁹ If any of the previously mentioned support would “involve costs to the City outside of their normal costs for employees performing their normal job duties, PredPol agrees to reimburse City for such costs. For example, if a Chief is requested to attend and speak at a conference of Police Chiefs to which they are not already traveling, PredPol agrees to reimburse City for travel expenses, if requested.”¹⁵⁰ The document is marked “CONFIDENTIAL” at the bottom.¹⁵¹

140. *Id.*

141. *Id.*

142. *Id.*

143. *Id.*

144. *Id.* The city of Columbia is referenced at several points in the contract. It is not clear why one reference is comparative and the other appears to be a mistake in the contract.

145. PREDPOL, Registration No. 4299222, Specimen (Dec. 13, 2012).

146. *Id.*

147. *Id.*

148. *See id.*

149. *Id.*

150. *Id.*

151. *Id.*

Despite its apparent contractual agreement to support PredPol, the Richmond Police Department terminated its relationship with the company in 2016, midway through a multi-year contract, because the city found that there was no measurable impact on crime reduction.¹⁵² It does not yet appear that journalists and civil liberties organizations have filed public records requests to determine whether Richmond received any additional discounts on its PredPol contract or took advantage of PredPol's offer to reimburse travel expenses in exchange for "reasonably supporting" PredPol's research and development.

IV. CONCLUSION

If the public had known the details about the secret surveillance technologies tricking our cell phones, tracking our license plates, and telegraphing our prospective criminality, perhaps we could have refused these technologies' use before they became firmly rooted in our criminal legal system. Surveillance transparency is tricky, but we need it more than ever. How can we resist invasive surveillance technologies, created by corporations and embraced by law enforcement, when we are not aware of the threats? Using federal trademark filings to investigate existing and future surveillance technologies offers journalists, researchers, and civil society the opportunity to better understand dangerous surveillance technologies and, hopefully, energize the public to mount a resistance.¹⁵³ By using federal trademark filings for surveillance transparency, we can adopt one more way to resist an entrenched power dynamic: the watched can become watchers.

152. Emily Thomas, *Why Oakland Police Turned Down Predictive Policing*, MOTHERBOARD (Dec. 28, 2016), https://motherboard.vice.com/en_us/article/ezp8zp/minority-retort-why-oakland-police-turned-down-predictive-policing; David Robinson & Logan Koepke, *Stuck in a Pattern: Early Evidence on "Predictive Policing" and Civil Rights*, UPTURN (Aug. 2016), <https://www.upturn.org/reports/2016/stuck-in-a-pattern/>.

153. The author hopes that the public will also embrace tools that scan the USPTO database for new trademark filings for surveillance technology.

PLATFORMS, ENCRYPTION, AND THE CFAA: THE CASE OF *WHATSAPP V. NSO GROUP*

Jonathon W. Penney[†] & Bruce Schneier^{††}

ABSTRACT

End-to-end encryption technology has gone mainstream. But this wider use has led hackers, cybercriminals, foreign governments, and other threat actors to employ creative and novel attacks to compromise or work around these protections, raising important questions as to how the Computer Fraud and Abuse Act (CFAA), the primary federal anti-hacking statute, is best applied to these new encryption implementations. Now, after the Supreme Court recently narrowed the CFAA's scope in *Van Buren* and suggested it favors a code-based approach to liability under the statute, understanding how best to theorize sophisticated code-based access barriers like end-to-end encryption, and their circumvention, is now more important than ever.

In this Article, we take up these very issues, using the recent case *WhatsApp v. NSO Group* as a case study to explore them. The case involves a lawsuit launched in 2019 by WhatsApp and Facebook against the cybersecurity firm NSO Group, whose spyware has been linked to surveillance of human rights activists, dissidents, journalists, and lawyers around the world, as well as the death of *Washington Post* journalist Jamal Khashoggi. The lawsuit, brought under the CFAA, alleged NSO Group launched a sophisticated hack that compromised countless WhatsApp users—many of which were journalists and activists abroad. Despite these broader human rights dimensions, the lawsuit's reception among experts has been largely critical. We analyze WhatsApp's CFAA claims to bring greater clarity to these issues and illustrate how best to theorize encrypted platforms and networks under the CFAA. In our view, the alleged attack on WhatsApp's encrypted network is actionable under the CFAA and is best understood using what we call a network trespass theory of liability. Our theory and analysis clarifies the CFAA's application, will lead to better human rights accountability and privacy and security outcomes, and provides guidance on critical post-*Van Buren* issues. This includes setting out a new approach to theorizing the scope and boundaries of computer systems, services, and information at issue, and taking the intended function of code-based access barriers into account when determining whether circumvention should trigger liability.

DOI: <https://doi.org/10.15779/Z384B2X554>

© 2021 Jonathon W. Penney & Bruce Schneier. The views expressed in this Article are solely those of the co-authors.

† Research Fellow; Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto; Faculty Associate, Berkman-Klein Center for Internet & Society, Harvard University. The author played no part in the WhatsApp v. NSO Group lawsuit, nor any research it is based on.

†† Fellow and Lecturer, Belfer Center for Science and International Affairs, Harvard Kennedy School; Fellow, Berkman-Klein Center for Internet and Society, Harvard University.

TABLE OF CONTENTS

| | | |
|-------------|--|------------|
| I. | INTRODUCTION | 470 |
| II. | <i>WHATS APP V. NSO GROUP</i>..... | 480 |
| III. | CRITICISMS AND POST-VAN BUREN PROBLEMS..... | 483 |
| IV. | UNDERSTANDING THE ATTACK AS A NETWORK TRESPASS..... | 484 |
| | A. THEORIZING THE SCOPE OF THE RELEVANT “COMPUTER SYSTEM” .. | 487 |
| | B. CIRCUMVENTING THE CENTRAL CODE-BASED ACCESS BARRIER | 493 |
| | 1. <i>The Access Circumvented a Code-Based Access Barrier</i> | 494 |
| | 2. <i>The Attackers Knew of the Code-Based Access Barrier</i> | 495 |
| V. | A NETWORK TRESPASS THEORY OF LIABILITY | 499 |
| | A. THE CFAA’S POLICY AIMS..... | 499 |
| | B. BETTER PRIVACY AND SECURITY OUTCOMES..... | 500 |
| | C. CORPORATE ACCOUNTABILITY FOR HUMAN RIGHTS VIOLATIONS ... | 504 |
| | D. IMPLICATIONS: <i>VAN BUREN</i> AND BEYOND..... | 506 |
| | 1. <i>Taking the Scope of the Computer System or Service Seriously</i> | 506 |
| | 2. <i>Theorizing and Defining Access Barrier Circumvention</i> | 508 |
| VI. | CONCLUSION | 510 |

I. INTRODUCTION

Encryption has gone mainstream.¹ Now, after the Snowden and Cambridge Analytica scandals showed there is a demand for it, smartphone manufacturers and social media companies have increasingly sought to employ encryption to ensure users’ privacy and security.² For example, popular social media messaging applications like WhatsApp, Facebook Messenger, Apple’s iMessage, Snapchat, and Zoom, among many others, all

1. Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 990 (2018).

2. Naomi Colvin, *Whistle-Blowing as a Form of Digital Resistance*, 7 STATE CRIME J. 24, 27 (2018) (“In making the covert visible, Edward Snowden’s revelations about mass surveillance also produced a recognition that there is a market for communications privacy. The proliferation of encrypted messaging applications and moves towards ubiquitous web encryption is a significant example of technical self-help against pervasive passive surveillance.”); Steven H. Hazel, *Privacy Self-Help*, 36 BERKELEY TECH. L.J. 305, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3623569 (noting “millions” of consumers engage in privacy self-help now, including using encrypted messaging apps); Ken Kantzer, *Yet Another End-To-End Encrypted App*, PKC SECURITY (Dec. 16, 2016), <https://www.pkcsecurity.com/yet-another.html> (“It seems that every week, yet another end-to-end encrypted app is unleashed on the world . . .”); Ariel Mahlmann, *End-to-End Encryption Strategies Becoming the Norm for Social Media*, FORNETIX (January 24, 2019), <https://blog.fornetix.com/end-to-end-encryption-strategies-becoming-the-norm-for-social-media>.

now implement end-to-end encryption or plan to do so in the near future.³ End-to-end encryption is a type of secure communications that ensures messages are entirely encrypted while in transit so only the sender and the recipient have the special cryptographic keys to decrypt and view communications; to anyone else, including the network or platform operators themselves, they are indecipherable.⁴ In this way, end-to-end encryption acts as both a code-based barrier—protecting the content of communications from all third parties—and an authentication gate, as only the sender and recipient have the keys to decrypt and view each message. There is also an important human rights dimension to these developments. Social justice activists at home⁵ and human rights activists and dissidents abroad increasingly use end-to-end encrypted messaging applications like Signal and WhatsApp to protect themselves from government and corporate surveillance, malicious hackers, and cybercriminals alike.⁶

3. Mahlmann, *supra* note 2; Dylan Clarke & Syed Taha Ali, *End to End Security is Not Enough*, in SECURITY PROTOCOLS 260, 261 (Frank Stajano, Jonathan Anderson, Bruce Christianson & Vashek Matyáš eds., 2017); Catalin Cimpanu, *Zoom backtracks and plans to offer end-to-end encryption to all users*, ZDNET (June 17, 2020), <https://www.zdnet.com/article/zoom-backtracks-and-plans-to-offer-end-to-end-encryption-to-all-users/>.

4. See *A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?*, ELEC. FRONTIER FOUND. SURVEILLANCE SELF-DEFENSE GUIDE (Nov. 19, 2018), <https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work>; Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?*, WIRED (Nov. 25, 2014, 9:00 AM), <https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/>; Leonid Grinberg, *End-to-End Authentication: A First Amendment Hook to the Encryption Debate*, 74 N.Y.U. ANN. SURV. AM. L. 173, 180–85 (2018); Mahlmann, *supra* note 2. For example, WhatsApp’s end-to-end encryption ensures only the sender and recipient can see communications—not any third parties, including other WhatsApp users or WhatsApp administrators themselves. See *About End-to-End Encryption*, WHATSAPP, <https://faq.whatsapp.com/general/about-end-to-end-encryption> (last visited Aug. 12, 2021).

5. Amelia Nierenberg, *Signal Downloads Are Way Up Since the Protests Began*, N.Y. TIMES (June 11, 2020), <https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html>.

6. See Colvin, *supra* note 2, at 35 (stating the UN Special Rapporteur for Freedom of Expression has also advocated for legal protections for encryption); Amelia Nierenberg, *Signal Downloads Are Way Up Since the Protests Began*, N.Y. TIMES (June 11, 2020), <https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html>; *Encryption is for “Real People”*, HUMAN RIGHTS WATCH DISPATCHES (Aug. 2, 2017), <https://www.hrw.org/news/2017/08/02/encryption-real-people> (“Who else uses end-to-end encryption? The list is long. Peaceful pro-democracy and reform activists in places like Hong Kong, Turkey, Central Africa, and across the Middle East. LGBT people living in countries where their sexual orientation is criminalized. Whistleblowers who reveal governmental or corporate malfeasance. Journalists everywhere trying to protect their sources. Add to that list diplomats and government officials, including some in the UK parliament and Foreign Office. Or doctors, lawyers, and business people discussing sensitive and confidential information.”).

But this wider use of encryption, especially in popular communications applications and networks, has led both governments and hackers to employ creative and novel methods to circumvent or “workaround” these protections, like exploiting encryption vulnerabilities or backdoors,⁷ or targeting communication network “endpoints” with malware and spyware.⁸ These activities raise important questions as to how the Computer Fraud and Abuse Act (CFAA), the primary federal anti-hacking statute, best applies to end-to-end encrypted networks and attempts to circumvent it. In fact, the issue has taken on even greater urgency in light of the United States Supreme Court’s recent landmark decision in *United States v. Van Buren*.⁹ The Court at long last endorsed a “narrow reading” of the CFAA, confirming it is “fundamentally” a trespass statute.¹⁰ That is, the “basic wrong” leading to

7. JEFF KOSSEFF, CYBERSECURITY LAW 336 (2020); Kerr & Schneier, *supra* note 1, at 1006; Nicole Perlroth, *What Is End-to-End Encryption? Another Bull’s-Eye on Big Tech*, N.Y. TIMES (Nov. 9, 2019), <https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html> (“[S]ecurity experts noted that any back door created for United States law enforcement agencies would inevitably become a target for foreign adversaries, cybercriminals and terrorists.”).

8. Clarke & Ali, *supra* note 3, at 261; Megan Squire, *End-to-End Encryption Isn’t Enough Security for “Real People”*, SCI. AM. (Aug. 15, 2017), <https://www.scientificamerican.com/article/end-to-end-encryption-isn-t-enough-security-for-ldquo-real-people-rdquo/>.

9. *Van Buren v. United States*, 141 S. Ct. 1648 (2021).

10. Orin Kerr, *The Supreme Court Reins In the CFAA in Van Buren*, LAWFARE BLOG (June 9, 2021), <https://www.lawfareblog.com/supreme-court-reins-cfaa-van-buren> (“[T]his is a major victory for those of us who favor a narrow reading of the CFAA. It settles that the CFAA is fundamentally a trespass statute. The basic wrong is bypassing a closed gate, going where you’re not supposed to go. The CFAA does not make it a crime to break a promise online. It does not make it a crime to violate terms of service. The statute is all about gates: When a gate is closed to a user, the user can’t wrongfully bypass the gate.”); *see also* Aaron Mackey & Kurt Opsahl, *Van Buren is a Victory Against Overbroad Interpretations of the CFAA, and Protects Security Researchers*, EFF DEEPLINKS BLOG (June 3 2021), <https://www.eff.org/deeplinks/2021/06/van-buren-victory-against-overbroad-interpretations-cfaa-protects-security>; *Van Buren: The implications of what is left unsaid*, IAPP PRIVACY ADVISOR (June 18, 2021), <https://iapp.org/news/a/van-buren-the-implications-of-what-is-left-unsaid/>; Will Duffield, *Van Buren Decision Is a Step in the Right Direction*, CATO INST. BLOG (June 14, 2021), <https://www.cato.org/blog/van-buren-decision-step-right-direction>; Clifford R. Atlas, Jonathan L. Crook, Jason Christopher Gavejian, Joseph John Lazzarotti & Erik J. Winton, *Supreme Court Adopts Narrow Interpretation of Computer Fraud and Abuse Act*, MARTINDALE LEGAL LIBR. (June 4, 2021), https://www.martindale.com/legal-news/article_jackson-lewis-pc_2546923.htm; Debbie L. Berman, David Bitkower, April A. Otterberg, Shoba Pillay, Aaron R. Cooper, Andrew J. Plague & Eric Fleddermann, *SCOTUS Limits the Reach of the Computer Fraud and Abuse Act, with Implications for Cybersecurity, Trade Secrets Litigation, and Beyond*, LEXOLOGY (June 6, 2021), <https://www.lexology.com/library/detail.aspx?g=25ca11d7-1dff-4a69-a256-030b97c4cbca>; Tiana Demas, Kathleen Hartnett, John Hemann, Travis LeBlanc, Joseph Mornin & Darina Shtrakhman, *US Supreme Court Narrows Scope of Computer Fraud and Abuse Act in Van Buren, Remands LinkedIn*, COOLEY

criminal and civil liability under the CFAA is bypassing an access barrier—or “gate”—in order to access, or go where you are not supposed to go, on a computer system or network.¹¹ Though the Court did not entirely settle what qualifies as a gate, it is clear the Court favors code-based or technological access restrictions—like end-to-end encryption.¹² Additionally, the Court cast considerable doubt on the usefulness of the CFAA in regulating and policing insider threats—those with authorization or permission to access a computer system or network—like an employee, contractor, or social media platform user who has created a free account.¹³ Insider threats have long been a central cybersecurity concern,¹⁴ especially in an era of ubiquitous computing and social media.¹⁵ Using what the Court called a “gates up-or-down inquiry,” if a

CYBER/DATA/PRIVACY INSIGHTS (June 9, 2021), <https://cdp.cooley.com/us-supreme-court-narrows-scope-of-computer-fraud-and-abuse-act-in-van-buren/>.

11. See *Van Buren*, 141 S. Ct. at 1651–58, 1661–62; Kerr, *supra* note 10; see also Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10. Certain leading scholars have long argued trespass law is key to understanding the CFAA. See, e.g., Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1146 (2016) (“[C]oncepts of authorization rest on trespass norms.”); Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477 (2016); Michael J. O’Connor, *The Common Law of Cyber-Trespass*, 85 BROOK. L. REV. 421, 434–35 (2019).

12. In footnote 8 of *Van Buren*, the Court appears to leave open the possibility that contract and policy-based access restrictions can lead to CFAA liability despite rejecting the policy-based *use* restrictions at issue in the case. See 141 S. Ct. at 1658 n.8; see also Kerr, *supra* note 11; Orin Kerr (@OrinKerr), TWITTER (June 3, 2021, 8:10 PM), <https://twitter.com/OrinKerr/status/1400500114569916422> (concluding that *Van Buren* likely requires a “mostly technological test, but one that can be impacted by written restrictions”); Paul Ohm (@PaulOhm), TWITTER (Jun. 3, 2021, 5:57pm), <https://twitter.com/paulohm/status/1400466767290400784> (“I think footnote 8 is a red herring and just forestalls the eventual ‘code-based’ approach in some future opinion. It’s hard to read the rest of the opinion without thinking Barrett is gesturing requiring code-based.”); Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10.

13. The Court called them “inside hackers.” *Van Buren*, 141 S. Ct. at 1658.

14. Indeed, most cybercrime is committed by “insiders.” See Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1493 (2016) (noting in Table 4 that well over half of cybercrime was committed by a combination of employees, consultants, and contractors, users or customers, and business partners); Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA HIGH TECH. L.J. 177, 184 (2000) (“According to recent FBI assessments, disgruntled insiders are a principal source of computer crimes.”); see also LUCAS WRIGHT, PEOPLE, RISK, AND SECURITY 40–43 (2017) (discussing insider threats).

15. Popular social media and communications platforms (like Facebook, Twitter, or WhatsApp) typically have hundreds of millions, even billions, of users—a target rich environment for malicious actors—and are generally accessible to anyone with an internet connection. See Marianna Noll, *Insider Threats on Social Media*, IT SECURITY CENTRAL (November 7, 2017), <https://itsecuritycentral.teramind.co/2017/11/07/insider-threats-on-social-media/> (“Consider how much compromising information people share on social media which can include personal life details, political views, location, interests, and much

user has any authorized access to a computer system (“gates up”) then there is no CFAA liability for violating *use* restrictions—like those found in terms of service or use policy—that regulate improper uses of the network or information therein to which they have access.¹⁶ Previously, if terms of service or use policies prohibited such activities—such as abusing access to target other users, misappropriating information for malicious purposes, or carrying out attacks or other illicit activities against targets elsewhere online—some courts found that insiders could be liable under the CFAA for exceeding their authorized access.¹⁷ Not anymore. Now, the only way an insider can exceed authorized access is when they access information—such as “files, folders, or databases,” etc.—in other “areas within the [computer] system,” to which they had no access to begin with.¹⁸

After *Van Buren*, understanding and theorizing the nature and scope of sophisticated code-based access barriers and authentication gates—like end-to-end encryption—under the CFAA is now more important than ever, as

more. For cyber criminals this data about a target is an absolute goldmine. . . . More than sharing information, social media platforms also provide another vector for phishing and drive-by-installations of malware. In either case social media platforms become a threat to your organization, which cannot be ignored if you allow your employees to use their social media at work.”); Ellen Messmer, *Hackers use corporate attacks as staging grounds for other cyber assaults*, NETWORK WORLD (Mar. 1, 2013), <https://www.networkworld.com/article/2164029/hackers-use-corporate-attacks-as-staging-grounds-for-other-cyber-assaults.html>; Guerrino Mazzarolo, Juan Carlos Fernández Casas, Anca Delia Jurcut & Nhien-AnLe-Khac, *Protect Against Unintentional Insider Threats: The risk of an employee’s cyber misconduct on a Social Media Site*, in CYBERCRIME IN CONTEXT 79–82 (M. Kranenborg & Leukfeldt eds., 2021); see also Helen Margetts, *Rethinking Democracy With Social Media*, in RETHINKING DEMOCRACY 107–08 (Andrew Gamble & Tony Wright eds., 2019) (“Social media—digital platforms which allow the creation, location and exchange of content—are entwined with every democratic institution and the daily lives of citizens, having reached incredible levels of penetration. Worldwide, Facebook has 2 billion users, YouTube has 1.5 billion, Whats-App 1.2 billion, Instagram 700 million, Twitter 328 million and the Chi-nese WeChat 889 million; nearly three quarters (73 per cent) of US adults use YouTube, while 68 per cent use Facebook.”).

16. *Van Buren*, 141 S. Ct. at 1651–58, 1661–62; Kerr, *supra* note 10; Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10.

17. There was a significant Circuit split before *Van Buren*. This broader interpretation of the CFAA—that breaching use policies could lead to liability—was held by the First, Fifth, Seventh, and Eleventh Circuits. The “narrow interpretation” of the CFAA, employed by the Second, Fourth, and Ninth Circuits, largely held that CFAA liability requires something more than a mere use restriction violation, like those found in terms of service or use policies. See KOSSEFF, *supra* note 7, at 176–83; Jonathan Mayer, *The “Narrow” Interpretation of the Computer Fraud and Abuse Act: A User Guide for Applying United States v. Nosal*, 84 GEO. WASH. L. REV. 1644, 1646, 1657–58 (2016).

18. *Van Buren*, 141 S. Ct. at 1651–59, 1662; Kerr, *supra* note 10; Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10.

well as efforts to circumvent them by insiders with network access.¹⁹ But just as important is the task of theorizing different kinds of computer systems, and information therein, under the CFAA to understand what it means for users to exceed authorized access by accessing “information” in “other areas” within a “computer system.”²⁰ Theorizing the nature of the computer system and the misappropriated information at stake has always been an important issue under the CFAA,²¹ but after *Van Buren*, it is now central to any CFAA liability analysis, particularly concerning hackers with authorized access to a network. Yet, this is an issue that courts have often failed to address seriously or systematically.²²

In this Article, we take up these very issues, using a recently launched lawsuit *WhatsApp v. NSO Group*,²³ as a case study to explore them. The lawsuit was brought by WhatsApp Inc. and its parent company, Facebook, pursuing multiple CFAA claims against the cybersecurity firm NSO Group and its parent company Q Cyber Technologies (hereinafter “Complaint”).²⁴ The Complaint, filed in California, alleged among other things that in 2019 NSO Group exploited a vulnerability in WhatsApp in order to spy on and monitor WhatsApp users, violating several provisions under the CFAA. WhatsApp CEO Will Cathcart, in launching the suit, declared it was part of the company’s efforts to “protect the privacy and security of our users

19. Bryan Cunningham, John Grant & Chris Jay Hoofnagle, *Fighting Insider Abuse After Van Buren*, LAWFARE BLOG (June 11, 2021), <https://www.lawfareblog.com/fighting-insider-abuse-after-van-buren>; Timothy Edgar, *Why Van Buren Is Good News for Cybersecurity*, LAWFARE BLOG (August 4, 2021), <https://www.lawfareblog.com/why-van-buren-good-news-cybersecurity>.

20. Atlas et al., *supra* note 10 (noting that the key inquiry under the CFAA involves determining whether an individual had authorized access to the “areas of a computer system at issue”); Cunningham, Grant & Hoofnagle, *supra* note 19.

21. Mayer, *supra* note 17, at 1651–53 (observing that “order to properly evaluate these theories of liability, a court must necessarily sketch the boundaries of the computer system and the information and services that the defendant accessed”); Orin S. Kerr, *Cybercrime’s Scope: Interpreting Access and Authorization in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1653 (2003).

22. Mayer, *supra* note 17, at 1651–53 (noting that “courts have not seriously defined the scope of a computer system”); Kerr, *supra* note 21, at 1653 (noting the *Morris* case “raised questions about how to divide a network of computers into individual computers for the purpose of the statute,” though those issues were ignored by the Second Circuit on appeal).

23. Complaint & Demand for Jury Trial at 1, WhatsApp, Inc. & Facebook, Inc. v. NSO Grp. Technologies Ltd. & Q Cyber Technologies Ltd., No. 3:19-cv-07123, 2015 WL 1033734 (N. D. Cal. Oct. 29, 2019) [hereinafter Complaint].

24. *Id.* at 11–13.

everywhere.”²⁵ Indeed, the case has important implications for privacy, security, and human rights, and not just due to WhatsApp’s massive 1.6 billion active user base.²⁶ NSO Group’s Pegasus spyware tool has been directly linked to surveillance of human rights activists, dissidents, journalists, and lawyers in countries around the world—often by governments with poor human rights records—as well as the death of *Washington Post* journalist Jamal Khashoggi.²⁷ More recently, the Pegasus Project, publicized by Amnesty International, documented 50,000 Pegasus spyware targets—via methods that echoed the 2019 attack on WhatsApp users—linking NSO Group to the surveillance of countless heads of state, human rights activists, and journalists globally, including Jamal Khashoggi’s family.²⁸ But the case also goes to the heart of ambiguities as to how encrypted networks, like WhatsApp’s end-to-end encryption service, are best theorized under the CFAA, a salient issue given the broad range of online service providers and platforms now incorporating this technology. Moreover, the FBI is investigating NSO Group for CFAA violations due to the WhatsApp hack, which means criminal proceedings may also follow regardless of what happens in the civil litigation.²⁹

25. Will Cathcart, *Why WhatsApp is pushing back on NSO Group hacking*, WASH. POST (Oct. 29, 2019), <https://www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/>.

26. Simon Kemp, *Digital 2020: Global Digital Overview*, DATAREPORTAL (Jan. 30, 2020), <https://datareportal.com/reports/digital-2020-global-digital-overview>.

27. Many such links have been made via research by the Citizen Lab, based at the University of Toronto’s Munk School of Global Affairs and Public Policy. *See NSO Group*, CITIZEN LAB, <https://citizenlab.ca/tag/nso-group/> (last visited Sept. 17, 2021) (supplying links to reports and related media); *see also* Nina dos Santos & Michael Kaplan, *Jamal Khashoggi’s private WhatsApp messages may offer new clues to killing*, CNN (Dec. 4, 2018), <https://www.cnn.com/2018/12/02/middleeast/jamal-khashoggi-whatsapp-messages-intl/index.html>.

28. Stephanie Kirchgaessner, *Officials who are US allies among targets of NSO malware, says WhatsApp chief*, THE GUARDIAN (July 24, 2021), <https://www.theguardian.com/technology/2021/jul/24/officials-who-are-us-allies-among-targets-of-nso-malware-says-whatsapp-chief> (“Cathcart said that he saw parallels between the attack against WhatsApp users in 2019—which is now the subject of a lawsuit brought by WhatsApp against NSO—and reports about a massive data leak that are at the centre of the Pegasus project.”); Press Release, *Massive data leak reveals Israeli NSO Group’s spyware used to target activists, journalists, and political leaders globally*, AMNESTY INT’L (July 18, 2021), <https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/>; Ben Hubbard, *Someone Tried to Hack My Phone. Technology Researchers Accused Saudi Arabia*, N.Y. TIMES (Jan. 28, 2020), <https://www.nytimes.com/2020/01/28/reader-center/phone-hacking-saudi-arabia.html>.

29. Joseph Menn & Jack Stubbs, *Exclusive: FBI probes use of Israeli firm’s spyware in personal and government hacks—sources*, REUTERS (Jan. 30, 2020), <https://www.reuters.com/article/us-usa-cyber-nso-exclusive/exclusive-fbi-probes-use-of-israeli-firms-spyware-in-personal-and-government-hacks-sources-idUSKBN1ZT38B>.

Despite these broader human rights dimensions, the lawsuit's reception among experts has been largely critical. It has been derided as an exercise in public relations,³⁰ and the lawsuit's CFAA claims criticized by various legal and cyber-security experts as "muddled,"³¹ unclear, and "odd."³² Critics also argue the lawsuit's claims rely too heavily on terms of service (TOS) violations,³³ contrary to the "narrow interpretation" of the CFAA then employed by various Circuit Courts of Appeal, and recently endorsed by the Supreme Court in *Van Buren*.³⁴ But perhaps the most serious charge is that the lawsuit asserts a problematic interpretation of the CFAA. It alleges NSO Group is liable for exceeding authorized access to the WhatsApp messaging network not because the network was hacked or exploited but because it was the staging ground and conduit through which the Defendants carried out their alleged attack on WhatsApp users.³⁵ This "theory" of the CFAA claims, critics allege, is akin to arguing you need Google's permission before sending an email through Gmail's network servers.³⁶ If correct, they argue, then the internet itself is in trouble—it would mean CFAA liability every time a server, host, or network is used without permission or for activities not

30. Jamie Condliffe, *The Week in Tech: WhatsApp's Spyware Fight Is at Least Good P.R.*, N.Y. TIMES (Nov. 1, 2019), <https://www.nytimes.com/2019/11/01/technology/whatsapp-nso.html>.

31. Tor Ekeland, *What's Up with WhatsApp: Thoughts on the NSO CFAA Complaint*, TOR EKELAND L. BLOG (Oct. 30, 2019), <https://www.torekeland.com/whats-up-with-whatsapp-thoughts-on-the-nso-cfaa-complaint/>.

32. Condliffe, *supra* note 30 (quoting Susan Landau calling it "odd"); Newsroom, *Facebook Enters Uncharted Legal Waters With Spyware Suit*, FORDHAM L. NEWS (Nov. 1, 2019), <https://news.law.fordham.edu/blog/2019/11/11/facebook-enters-uncharted-legal-waters-with-spyware-suit/> (describing it as "risky").

33. See Andy Greenberg, *WhatsApp's Case Against NSO Group Hinges on a Tricky Legal Argument*, WIRED (Oct. 29, 2019), <https://www.wired.com/story/whatsapp-nso-group-lawsuit/> (interviewing Tor Ekeland).

34. See Mayer, *supra* note 17, at 1646, 1657–58; KOSSEFF, *supra* note 7, at 176–78.

35. Josephine Wolff, *Whatever You Think of Facebook, the NSO Group Is Worse*, N.Y. TIMES, (Nov. 6, 2019), <https://www.nytimes.com/2019/11/06/opinion/whatsapp-nso-group-spy.html> ("WhatsApp does its best to argue that NSO gained access to its own signaling and relay servers without authorization in the process of contacting WhatsApp users, but this is a dicey interpretation of the Computer Fraud and Abuse Act, akin to arguing that you need Google's permission to send an email to a Gmail user through Google's servers"); Ekeland, *supra* note 31 (arguing the Complaint reads as if there was "unauthorized access" because the Plaintiffs "didn't like the way their network was used" and insisting that "if that's the standard for CFAA liability . . . then most of the internet is in trouble").

36. Wolff, *supra* note 35.

authorized by administrators or owners.³⁷ Such a broad interpretation of the CFAA is, they argue, “dicey,”³⁸ “risky,”³⁹ and “dangerous.”⁴⁰

We analyze WhatsApp’s CFAA claims to bring greater clarity to these issues and illustrate how best to theorize encrypted networks and attacks on them under the CFAA. On the facts of the case, a fairly straightforward application of the CFAA would find that the Defendants were liable to targeted WhatsApp users for accessing their devices without authorization, using the WhatsApp network as a conduit to deliver malicious code to the victims’ smartphones that allowed the Defendants unauthorized access. In fact, that is the basis for much of the criticisms of the lawsuit—the targeted users were the proper plaintiffs. The harder question, which we tackle in this Article, is whether WhatsApp, the company, also has a CFAA claim against the Defendants for their alleged attack on WhatsApp’s encrypted messaging network. In our view, it does, based on what we call a network trespass theory.⁴¹ This theory of liability is simple. It holds accessing a network and using it to hack or stage an attack on users of that network—like obtaining unauthorized access to their personal computing devices using malicious code over the network—is a trespass not just on the individual devices of the targeted users, but on the network itself, and should attract liability under the CFAA.

This theory involves subtle two legal and theoretical shifts. First, we argue for a different theoretical understanding and scope of the “computer system” at issue here—WhatsApp’s encrypted communications network. Rather than theorizing user devices—through which users interface with the network via a software client—as separate computer systems, we argue they ought to be treated as constitutive of the same network for the purposes of determining CFAA liability. Typically, we think of computer networks—like the internet—as simply a series of interconnected but separate computers.⁴²

37. See Ekeland, *supra* note 31; Wolff, *supra* note 35.

38. Wolff, *supra* note 35.

39. Newsroom, *supra* note 32.

40. See Tim Cushing, *Malware Marketer NSO Group Looks Like It’s Blowing Off Facebook’s Lawsuit*, TECHDIRT (Jan. 15, 2020), <https://www.techdirt.com/articles/20200109/11485043708/malware-marketer-nso-group-looks-like-blowing-off-facebooks-lawsuit.shtml>; see also Alan Z. Rozenshtein, *The WhatsApp-NSO Group Lawsuit and the Limits of Lawful Hacking*, LAWFARE BLOG (Nov. 5, 2019), <https://www.lawfareblog.com/whatsapp-nso-group-lawsuit-and-limits-lawful-hacking>.

41. The theory is based on norms of trespass law as applied to certain kinds of online networks. See Kerr, *supra* note 11, at 1146 (“[C]oncepts of authorization rest on trespass norms.”); O’Connor, *supra* note 11, at 434–35; see generally Goldfoot & Bamzai, *supra* note 11.

42. MICROSOFT COMPUTER DICTIONARY 12 (4th ed. 1999) (defining it as “[a] group of computers and associated devices that are connected by communications facilities . . .”);

Hence, critics of *WhatsApp v. NSO Group* lawsuit claim the *real* victims of the hack are the users whose personal devices—separate computers from the WhatsApp network—were compromised and accessed. We argue this assumption makes sense for open networks like the internet but not encrypted networks like WhatsApp. End-to-end encrypted networks are not analogous to the open internet. They are closed networks with a central code-based design feature—end-to-end encryption—built into the network to protect the privacy and security of users and their communications. And users and their personal computing devices are not separate from the network, but, as the end nodes of the network that initiate, encrypt, send, receive, and decrypt calls, messages, and other user files and information shared over the network—essentially, all the core network functions—they are central to the network. As such, the scope and boundaries of the computer system here—the WhatsApp network—are best theorized as including users and their devices. Second, we argue that in deciding whether a code-based access barrier or authentication gate is circumvented or violated, courts should take into account the code-based access barrier’s *intended function* in a computer system or network. Leading scholars have long argued that the best way to approach code-based access restrictions is as authentication gates,⁴³ and there are passages in *Van Buren* suggesting the Supreme Court may favor such an approach.⁴⁴ But, we argue, construing code-based access barriers so narrowly may mean certain kinds of sophisticated attacks that “work around” stronger code-based barriers like encryption, in ways unrelated to authentication functions, may not trigger liability. To catch those too, we suggest that the *intended function* of the code-based barrier in a computer system or network should be taken into account, and where access is outside authentication or *inconsistent with the intended function of the authentication gate or code-based access barrier*, then the circumvention should trigger liability.

Analyzed through the lens of this network trespass theory, the facts alleged in the lawsuit support multiple violations under the CFAA. Our network trespass theory clarifies the CFAA’s application to communications networks. It is also consistent with the CFAA’s underlying trespass norms, ultimately avoids reliance on terms of service violations, and, we argue, should lead to better privacy and security outcomes in the long term. Second,

DICTIONARY OF COMPUTING 5 (6th ed. 2008) (defining it as “the shared use of a series of interconnected computers, peripherals and terminals”).

43. Kerr, *supra* note 11, at 1146; Kerr, *supra* note 10.

44. *Van Buren v. United States*, 141 S. Ct. 1648, 1651–59, 1662 (2021); Kerr, *supra* note 10; Mackey & Opsahl, *supra* note 10; Atlas et al., *supra* note 10; Berman et al., *supra* note 10.

the lawsuit helps fill a gaping void both domestically and internationally—a means to hold companies accountable for contributing to human rights abuses abroad. Lastly, though the WhatsApp lawsuit provides the foundation for our analysis, our arguments have implications far beyond it, providing guidance not just for FBI’s reported investigation of NSO Group for criminal CFAA violations, but also on critical post-*Van Buren* issues: theorizing the nature and scope of “computer systems” and “areas”—like encrypted communications networks and similar platforms—and how best to theorize sophisticated code-based measures like end-to-end encryption, and efforts to bypass it, under the CFAA.

Our analysis has two caveats. First, though the factual allegations in the Complaint are not yet proven—and NSO Group has disputed them in court filings⁴⁵—for the purposes of this Article, we assume the allegations set out are true. We also rely on some additional facts and research concerning WhatsApp’s vulnerability that were not pleaded in the action. Second, we also focus primarily on the CFAA legal claims set out in the Complaint. A fuller analysis of other issues—like WhatsApp’s claims under California state law or NSO Group’s jurisdictional arguments and sovereign immunity claims⁴⁶—would take us beyond the scope of this Article. However, our arguments have implications for WhatsApp’s claims under California’s Comprehensive Computer Data Access and Fraud Act and trespass law,⁴⁷ in addition to possible criminal violations being presently investigated. In Part II, we set out the central factual and legal claims in the lawsuit and then set out predominant criticisms. We then set out our network trespass theory in Part III, and argue that it is consistent with the CFAA’s intended trespass foundations, it is narrow, and it will lead to better privacy and security outcomes in the long term. We also examine broader human rights implications of our account in Part IV.

II. *WHATS APP v. NSO GROUP*

Before addressing criticisms, it makes sense to briefly discuss the allegations and their context. The Complaint sets out a range of factual and legal allegations against NSO Group and centers on a security vulnerability in

45. Defendants’ Motion for Summary Judgement at 2–8, WhatsApp, Inc. & Facebook, Inc. v. NSO Grp. Technologies Ltd. & Q Cyber Technologies Ltd., No. 3:19-cv-07123, 2015 WL 1033734, (N. D. Cal. Oct. 29, 2019).

46. *Id.* at 8–15.

47. Complaint, *supra* note 23, at 11–13; Greenberg, *supra* note 33 (quoting Riana Pfefferkor, cybersecurity expert at Stanford Law, noting the CFAA as the “main show” in the lawsuit).

the WhatsApp messaging service discovered in May 2019 and widely reported at the time⁴⁸ that exposed WhatsApp users to unauthorized tracking and surveillance. Facebook’s security advisory described the vulnerability as one exploited through “remote code execution” via “specially crafted series of RTCP packets” sent, via WhatsApp’s messaging network, to the phone numbers of targeted users.⁴⁹ Put in less technical terms, the attackers sent malicious code over the WhatsApp message service network that was specially designed to exploit a flaw in the network.⁵⁰ This malicious code, which could be delivered simply by virtue of a missed phone call without any interaction by victims, triggered the download of spyware onto targets’ phones.⁵¹ The spyware gave the attackers full access and control over victims’ smartphones remotely, including access to messages that they normally could not access because of WhatsApp’s end-to-end encryption as well as files, emails, call logs, text messages, photos, and videos—in short, everything.⁵² The spyware, according to reports, bore all the hallmarks of NSO Group’s Pegasus spyware tool.⁵³ After the lawsuit was filed, Citizen Lab issued a statement regarding research it had done linking NSO Group and the Pegasus spyware to the attack and identifying over one hundred cases of human rights defenders victimized globally, including civil society groups, activists, lawyers, and journalists located throughout the world.⁵⁴

This is essentially what is alleged in the lawsuit, with a few additional technical insights as how the attack was carried out. First, the Complaint asserts that NSO Group (“the Defendants”) created “various WhatsApp

48. Mehul Srivastava, *WhatsApp voice calls used to inject Israeli spyware on phones*, FIN. TIMES (May 13, 2019), <https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab?>; Julia Carrie Wong, *WhatsApp urges users to update app after discovering spyware vulnerability*, THE GUARDIAN (May 14, 2019), <https://www.theguardian.com/technology/2019/may/13/whatsapp-urges-users-to-upgrade-after-discovering-spyware-vulnerability>; Nick Hopkins & Stephanie Kirchaessner, *WhatsApp sues Israeli firm, accusing it of hacking activists’ phones*, THE GUARDIAN (Oct. 29, 2019), <https://www.theguardian.com/technology/2019/oct/29/whatsapp-sues-israeli-firm-accusing-it-of-hacking-activists-phones>.

49. *Security Advisory*, FACEBOOK (Aug. 13, 2019), <https://www.facebook.com/security/advisories/cve-2019-3568>; *The NSO WhatsApp Vulnerability—This is How It Happened*, CHECK POINT RES. (May 13, 2019), <https://research.checkpoint.com/2019/the-nso-whatsapp-vulnerability-this-is-how-it-happened/>.

50. CHECK POINT RES., *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

51. CHECK POINT RES., *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

52. CHECK POINT RES., *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

53. CHECK POINT RES., *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

54. *NSO Group / Q Cyber Technologies Over One Hundred New Abuse Cases*, CITIZEN LAB (Oct. 29, 2019), <https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/>.

accounts,” “agreed” to the WhatsApp Terms of Service in doing so,⁵⁵ then “reverse-engineered” the WhatsApp app, and “developed a program to enable them to emulate legitimate WhatsApp network traffic.”⁵⁶ This was done in order to surreptitiously “transmit malicious code—undetected—to Target Devices over WhatsApp servers.”⁵⁷

Second, the Defendants “routed and caused to be routed” the malicious code through WhatsApp’s servers—including “Signaling Servers and Relay Servers—concealed within part of the normal network protocol.”⁵⁸ They then used, without authorization, the Signaling Servers to transmit the “malicious code” to the Target Devices, bypassing restrictions on the Signaling Servers and concealing the malicious code in normal call traffic.⁵⁹ The malicious code was “injected” into the memory of Target Devices, and the Defendants later used Relay Servers to send encrypted packets also designed to “activate” the malicious code installed in the memory of Target Devices, triggering them to download spyware controlled by the Defendants.⁶⁰

Third, the Complaint alleged the Defendants attempted to hack 1,400 different users worldwide in April and May 2019.⁶¹ Based on these facts, the Complaint asserts multiple claims under the CFAA, including that the Defendants intentionally accessed without authorization a protected computer; knowingly, and with intent to defraud, accessed a protected computer without authorization contrary to sections 1030(a)(2)), 1030(a)(4), and 1030(b); as well as various claims of damages and loss.⁶² We do not analyze each and every one of these claimed violations but focus on the central claims—whether the attackers either accessed without authorization or exceeded authorized access.

55. Complaint, *supra* note 23, at 7.

56. *Id.* at 8.

57. *Id.*

58. *Id.* The WhatsApp messaging network implements a version of the WebRTC, or Web Real Time Communications, protocol. Under WebRTC, “relay servers” are servers that facilitate communications between users on the network when direct peer-to-peer connections are not possible, while signaling servers sent information over the network to help to initialize connections between users via the relay servers. See Ivan Drnasin, Mislav Grgic & Gordan Gledec, *Exploring WebRTC Potential for DICOM File Sharing*, 33 J. DIGITAL IMAGING 697, 698 (2019); Sam Dutton, *Getting Started with WebRTC*, HTML5 ROCKS BLOG (Feb. 21, 2014), <https://www.html5rocks.com/en/tutorials/webrtc/basics/>.

59. Complaint, *supra* note 23, at 8.

60. *Id.* at 8–9.

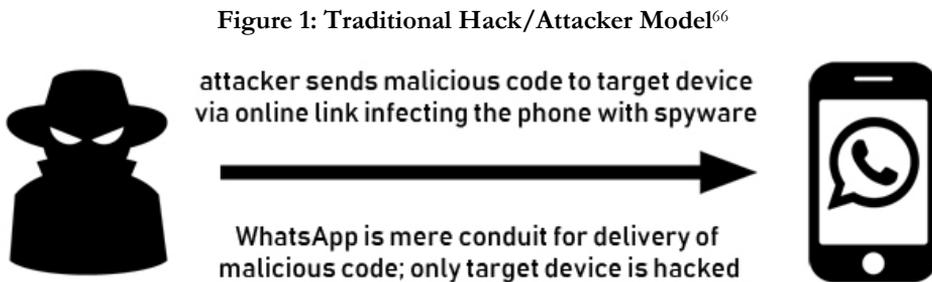
61. *Id.* at 9.

62. *Id.* at 10–11.

III. CRITICISMS AND POST-VAN BUREN PROBLEMS

The two most important criticisms concern the theoretical premises of the lawsuit itself. And both, in turn, have been strengthened by the Supreme Court’s decision in *Van Buren*. First, the lawsuit, critics allege, relies primarily on terms of service violations as a theory of CFAA liability.⁶³ If so, then that *would* be a serious problem as it would be inconsistent with the “narrow reading” of the CFAA endorsed by the Supreme Court in *Van Buren*.⁶⁴ Second, the lawsuit deploys a “risky” or dangerously broad interpretation of the CFAA by alleging the Defendants are liable for unauthorized access simply because they allegedly used that network in ways WhatsApp did not authorize or approve; on this angle of view, only the targeted WhatsApp users are the victims, not WhatsApp.⁶⁵

Each of these criticisms is based, to varying degrees, on a deeper theoretical understanding of the WhatsApp messaging network and the nature of the attack on WhatsApp users. This understanding or model of the attack is visualized in Figure 1, with an attacker focused on targeted users and WhatsApp merely a conduit for delivering the attacker’s malicious code to the target.



On this traditional model or understanding of the attack, the real victims here are the end users: those WhatsApp users whose smartphones were

63. See Ekeland, *supra* note 31; Greenberg, *supra* note 33 (quoting Ekeland and Pfefferkor); Condliffe, *supra* note 30 (quoting Ekeland and Pfefferkor).

64. Kerr, *supra* note 11, at 1146.

65. Wolff, *supra* note 35; Ekeland, *supra* note 31 (arguing the Complaint reads as if there was “unauthorized access” because the Plaintiffs “didn’t like the way their network was used,” and insists that “if that’s the standard for CFAA liability . . . then most of the internet is in trouble.”).

66. The spy icon in this figure was created by Hopstarter and its production here is licensed under CC BY 4.0. The smartphone icon is public domain and not restricted by copyright (CC0 1.0).

infected by malicious code that caused their devices to download and install spyware giving control to third parties—clients and customers of NSO Group, as the Complaint alleges. On this view, WhatsApp, by contrast, was not hacked. It was simply a conduit for the attack—analogue to the open internet—but has no recourse under the CFAA. There are at least three “computer systems” on this understanding: the sending WhatsApp user device; the WhatsApp network; and the receiving WhatsApp user device. On this view, the users, not WhatsApp, are the proper plaintiffs in the action, as it is their information on their personal devices accessed without authorization. Putting this understanding in the terms used by the Supreme Court in *Van Buren*, the alleged attackers here, who had access to the WhatsApp network, did not obtain or alter information in “other areas” of the computer system in which they had access.⁶⁷ Rather, they entered an entirely different computer system—the smartphones of targeted users.

This theoretical approach, in our view, misunderstands the nature of the attack and how best to theorize it under the CFAA.

IV. UNDERSTANDING THE ATTACK AS A NETWORK TRESPASS

As noted in the previous Part, courts and commentators have been divided over the scope and application of the CFAA⁶⁸ with multiple different approaches employed in case law and scholarship.⁶⁹ More recently, however, leading scholars and experts like Orin Kerr, Josh Goldfoot, and Aditya Bamzai have advanced a “trespass” theory of the CFAA as a means to unify existing case law, theory, and approaches on point.⁷⁰ Indeed, successive House Reports through the 1980s, which led to the CFAA’s enactment, described computer hacking, or unauthorized access to computer networks, as “trespassing” and described hackers to “trespassers.”⁷¹ A Senate Report that led to CFAA amendments in 1996 employed the same view, observing

67. *Van Buren v. United States*, 141 S. Ct. 1648, 1651–59, 1662 (2021); Kerr, *supra* note 10.

68. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1562 (2010).

69. Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1445 (2016); Kelsey T. Patterson, *Narrowing It Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 499 (2013).

70. Kerr, *supra* note 11; Goldfoot & Bamzai, *supra* note 11; *see also* O’Connor, *supra* note 11.

71. Goldfoot & Bamzai, *supra* note 11, at 1482.

that the CFAA “criminalizes all computer trespass.”⁷² More recently, courts have increasingly interpreted and applied the CFAA through a trespass framework⁷³ with the law’s central “unauthorized access” concept interpreted as reflecting the right to exclude others from accessing property in traditional trespass law.⁷⁴ And now, the Supreme Court has largely vindicated this approach in *Van Buren*.⁷⁵

A trespass framework also offers the best approach to theorize encrypted networks under the CFAA. But translating these largely settled physical trespass norms and requirements into computer and digital contexts—where they are largely unsettled—creates difficulties.⁷⁶ On this count, we agree with Kerr and others that a “code-based” standard offers the optimal means to operationalize trespass requirements in digital and computerized contexts.⁷⁷ That is, unauthorized access or exceeding authorized access is best understood under the CFAA as access to a computer that violates, breaks, by-passes, or circumvents a code-based restriction, barrier, or authentication gate. Put simply, the access barrier, restriction, or authentication gate violated by the trespasser on this interpretation is one implemented by the code, design, and architecture of the computer or the computer network accessed.⁷⁸ Indeed, based on *Van Buren*, it is likely the Supreme Court likewise favors a code-based approach to access restrictions, including in deciding if a user has exceeded authorized access to a computer network.⁷⁹

Employing a code-based approach to exceeding authorized access under the CFAA, our network trespass theory is simple. The WhatsApp messaging network’s central design feature is end-to-end encryption, which was incorporated in the messaging service to protect the privacy and security of user communications.⁸⁰ The WhatsApp messaging network’s central design

72. Goldfoot & Bamzai, *supra* note 11, at 1482; Kerr, *supra* note 11, at 1144 n.3.

73. Goldfoot & Bamzai, *supra* note 11, at 1482–83; Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1396 (2007).

74. Goldfoot & Bamzai, *supra* note 11, at 1478–79; Kerr, *supra* note 11, at 1144 n.3.

75. Kerr, *supra* note 10 (stating that the Supreme Court in *Van Buren* “settles that the CFAA is fundamentally a trespass statute”).

76. Kerr, *supra* note 11, at 1147.

77. See Kerr, *supra* note 11, at 1147 (articulating an “authentication gate” standard as offering the best balance between open internet norms and the CFAA’s trespass norms); Kerr, *supra* note 21, 1657–58 (advancing a “code-based restriction” interpretation of the CFAA’s liability standard); see also Bellia, *supra* note 69; Patterson, *supra* note 69, at 528 (“[C]ourts should expressly adopt a code-based approach to [the CFAA’s] interpretation.”).

78. See Goldfoot & Bamzai, *supra* note 11, at 1487–88 (discussing code-based restrictions).

79. See *supra* note 12.

80. Security, WHATSAPP, <https://www.whatsapp.com/security> (last visited Oct. 1, 2020) [hereinafter *WhatsApp Security*]; *About End-to-End Encryption*, WHATSAPP, <https://>

feature is end-to-end encryption, which was incorporated in the messaging service to protect the privacy and security of user communications.⁸¹ The attackers, alleged to be NSO Group, took steps—including spoofing WhatsApp client software, exploiting security vulnerabilities, and concealing and sending malicious code in normal network traffic via WhatsApp servers, thereby infecting WhatsApp user devices—in order to access user communications by circumventing the end-to-end encryption protecting them. In other words, the Defendants knew about a clear prohibition or code-restriction on access to user communications within the WhatsApp messaging network—the code-based end-to-end encryption—and violated that restriction by taking multiple steps to circumvent the encryption to access user communications, among other data. This is a trespass, on traditional trespass requirements, but not just on the users; but on the WhatsApp messaging network itself.

That sounds simple enough. But this network trespass theory involves two important but subtle legal and theoretical shifts in applying parts of the CFAA. First, we argue for a different theoretical understanding and scope of the “computer system” at issue here—WhatsApp’s encrypted communications network. Rather than theorizing user devices—through which users interface with the network via a software client—as separate computer systems, we argue they ought to be treated as constitutive of the same network for the purposes of determining CFAA liability. Typically, we think of computer networks—like the internet—as simply a series of interconnected but separate computers.⁸² This assumption actually underlies some of the central criticisms of the *WhatsApp v. NSO Group* lawsuit, which hold that the *real* victims of the hack are the users whose personal devices—separate computers from the WhatsApp network—were compromised and accessed. We argue this assumption makes sense for open networks like the internet but not encrypted networks like WhatsApp. Second, we argue that in

faq.whatsapp.com/en/general/28030015/?category=5245250 (last visited Oct. 1, 2020) [hereinafter *WhatsApp Faq*]; WHATSAPP ENCRYPTION OVERVIEW: TECHNICAL WHITE PAPER (2020), https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=2&_nc_sid=2fbf2a&_nc_ohc=U4i2iUSaMEwAX-X1U2J&_nc_ht=scontent.whatsapp.net&oh=15593989c0626cbf40856b6468164a7e&oe=601F0119 [hereinafter WHATSAPP ENCRYPTION]; WHATSAPP, <https://www.whatsapp.com> (last visited Oct. 1, 2020) [hereinafter WHATSAPP WEBSITE].

81. *WhatsApp Security*, *supra* note 80; *WhatsApp Faq*, *supra* note 80; WHATSAPP ENCRYPTION, *supra*, note 80; WHATSAPP WEBSITE, *supra*, note 80.

82. MICROSOFT COMPUTER DICTIONARY 12 (4th ed. 1999) (“A group of computers and associated devices that are connected by communications facilities”). A DICTIONARY OF COMPUTING 5 (6th ed. 2008) (“the shared use of a series of interconnected computers, peripherals and terminals”).

order to understand when a code-based access barrier or authentication gate has been circumvented to trigger liability, the *intended function* of the code-based barrier in a computer system or network should be taken into account. Focusing on only how a code-based measure authenticates users can miss how attackers formulate sophisticated attacks that, rather than tricking or compromising the authentication gate itself, wholly circumvents it. Such “work around” attacks are common particularly with stronger forms of code-based access barriers that are harder to trick, compromise, or hack—like encryption. Instead, attackers find a way to work around the barrier. That is essentially what the attackers did here according to the alleged facts, and it should trigger CFAA liability.

A. THEORIZING THE SCOPE OF THE RELEVANT “COMPUTER SYSTEM”

Our first task is to theorize the proper scope and boundaries of the relevant “computer system” at issue.⁸³ Defining the scope, boundaries, and areas of the computer system at issue here—the WhatsApp encrypted network, as well as the information accessed therein—is critical because depending on whether the targeted users are part of the network or not will impact whether the attackers exceeded any authorized access by accessing “other areas” within a “computer system.”⁸⁴ On this count, critics of the WhatsApp lawsuit argued the attackers were simply using the WhatsApp messaging network to target end-users⁸⁵ as if it was merely a conduit or staging ground for the attack. They also analogized WhatsApp to the open internet, a network over which the hack was staged but separate from the relevant computer system that was actually hacked—the targeted devices of users. As such, WhatsApp is not the victim, only targeted users. These are intuitive arguments because people access WhatsApp via their smartphones, and smartphones are themselves stand-alone personal computing devices. And we tend to think of computer networks as simply a series of connected but separate or individual computers with the internet being a key such example.⁸⁶

83. Mayer, *supra* note 17, at 1646.

84. Atlas et al., *supra* note 10 (noting that “[t]he key inquiry under the CFAA” involves determining whether an individual had authorized access to the “areas of a computer system at issue”); Cunningham, Grant & Hoofnagle, *supra* note 19.

85. Wolff, *supra* note 35; Ekeland, *supra* note 31 (arguing the Complaint reads as if there was “unauthorized access” because the Plaintiffs “didn’t like the way their network was used,” and insists that “if that’s the standard for CFAA liability . . . then most of the internet is in trouble”).

86. See *supra* note 82 and accompanying text.

This is important because, as alleged in the Complaint, the Defendants created accounts on the WhatsApp messaging network to carry out the attack.⁸⁷ So, it is likely the Defendants had “authorized access” to the WhatsApp network, at least initially,⁸⁸ and thus a key issue for CFAA liability is whether they “exceeded authorized access.”⁸⁹ That phrase is expressly defined in the statute to “access a computer with authorization” and to use that access to “obtain or alter information” that “in the computer” that the attacker is “not entitled so to obtain or alter.” That language—“in the computer”—means that exceeding authorized access involves hacking *in the computer system itself* and not using it as a staging ground or conduit for attacks on other computers, as critics argue. In other words, if we accept that WhatsApp user devices are separate computers from the WhatsApp network, any information obtained or altered on them are not “in the computer” or WhatsApp network, and thus attackers would not have exceeded their access and would not be liable.

Nevertheless, we believe a proper legal and technical understanding of the WhatsApp network would approach user devices as a key part of the network itself, and not separate. In determining the scope of the relevant computer system or service and the information therein for CFAA purposes, we agree with Jonathan Mayer that an “objective” approach that takes into account the perceptions of ordinary users is preferable.⁹⁰ However, we would also include two other factors in making this determination: the technical realities of the computer system, service, and information and the nature of the hack itself. In other words, what was the information the attackers were targeting and what was their methodology? Applying this approach, WhatsApp users and their devices should be theorized as central parts of the WhatsApp network, not separate computer systems.

First, an ordinary user would not only perceive the WhatsApp messaging network as one system as a whole—as our analysis has argues—but also that an individual account on that system constitutes a “distinct set of information.” This means, accessing other user accounts and their information would almost surely be understood by ordinary users as

87. Complaint, *supra* note 23, at 7–8.

88. Mayer, *supra* note 17, at 1646. Of course, it could also be argued that if they had created accounts *only* for the purpose of carrying out the attack, there was no permission or authorization at any stage.

89. 18 U.S.C. § 1030(a)(2)(C) (2018) (“Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section.”); 18 U.S.C. § 1030(e)(6).

90. See Mayer, *supra* note 17, at 1653.

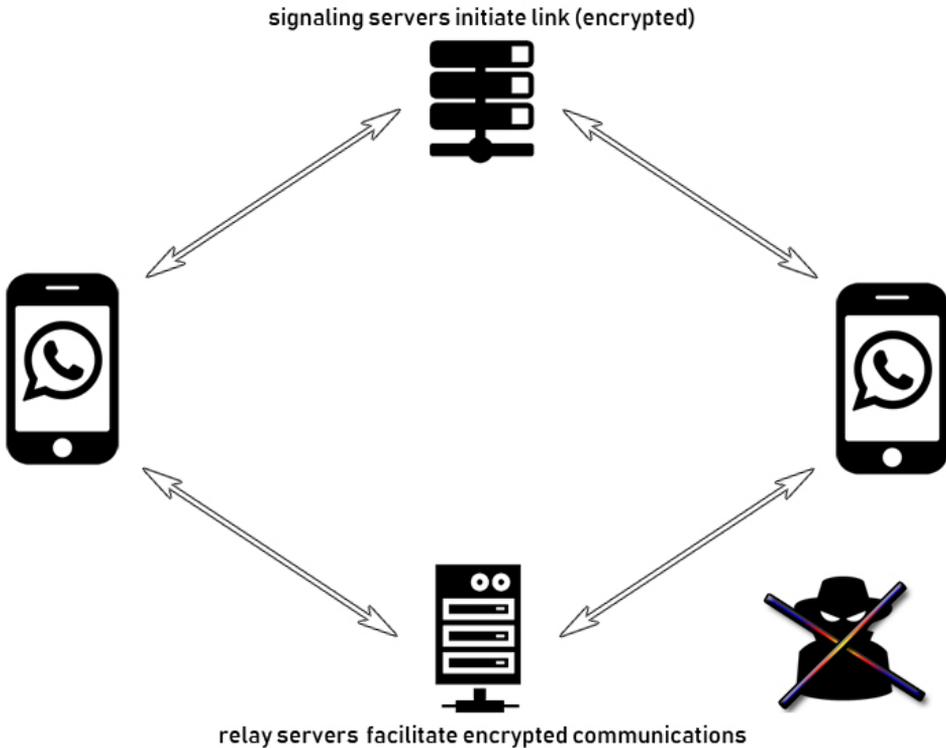
accessing “other areas” on the computer system to which their own authorized access would not extend. No reasonably or ordinary user would believe they would have access to the “information” of other users, like private messaging, data, media, files, and anything else shared via private chats. This is especially so given that WhatsApp promotes its end-to-end encryption as a central feature of the network that, as noted earlier, protects user messages, files, and information from other users, third parties, and from even WhatsApp itself. On this view, encryption is a clear code-based restriction on access to other user’s “information”—that is, communications within that network.⁹¹

Second, the technical realities of the WhatsApp messaging network confirm these ordinary user perceptions. In the WhatsApp network, users—who interface via smartphone devices running the WhatsApp client—are not peripheral or separate from the system, but core to the functions of the network itself. This is clear from a visualization of the network itself in Figure 2.⁹²

91. *Id.*

92. WHATSAPP ENCRYPTION, *supra* note 80, at 3, 11; *WhatsApp Security*, *supra* note 80.

Figure 2: The End-to-End Encrypted WhatsApp Network⁹³—The WhatsApp messaging network protects communications from third-party surveillance through end-to-end encryption.



Visualized in Figure 2, the notion of the WhatsApp messaging service *as a network* is clear. Included in the network are all WhatsApp users; their client applications (smartphone app or web-based); and a series of server nodes (Signal and Relay Servers) that initiate, coordinate, and facilitate all communications and data across the network. When a user drafts and sends a message on their WhatsApp client, it is immediately encrypted by the sender's client. This initiating or sending user's client then sends a request to the Signaling Servers to initiate an encrypted link between the sending user and the recipient user. Relay Servers also facilitate encrypted communication data transmissions between users, especially where obstacles such as firewalls exist. The Recipient's WhatsApp client receives encrypted messages, which

93. Both Figure 2 and Figure 3 were created drawing on alleged facts and details in the Complaint as well as on other related commentary, research, and documentation. *See supra* notes 3–33. The network server icons used in this figure are licensed under CC BY 4.0 by SVG Repo. The spy icon in this figure was created by Hopstarter and is licensed under CC BY 4.0. The smartphone icon is public domain and not restricted by copyright (CC0 1.0).

are then decrypted using both a public and private key. What is also clear from this visualization is that users are not peripheral to the messaging network, but core to its central function—communications. At the same time, the technical reality is consistent with ordinary user perceptions—each user account, client, or device, though part of the overall computer network or system, are nevertheless distinct elements of that network. Due to end-to-end encryption, users do not have access to the encrypted messages of any other users.

Furthermore, analogizing the WhatsApp messaging network to the open internet is incorrect, both legally and technically. The WhatsApp messaging network is not the open internet nor is it an open network or web service. First, the central design feature of WhatsApp’s messaging network is end-to-end encryption, a code-based barrier that encloses the entire network from outsiders seeking to intercept user communications. The internet’s fundamental architecture lacks this design feature—it is open and general.⁹⁴ This open and flexible architecture made communications and connectivity easier, but also made surveillance and eaves-dropping far easier as well.⁹⁵ Second, unlike the open internet or web, to use Kerr’s terms, not all visitors “get service.”⁹⁶ To access the network, a user must first create an account, agree to the TOS, and then download and install onto their device the authorized WhatsApp smartphone client apps or log into the authorized WhatsApp web-based client.⁹⁷ Finally, once accessing the WhatsApp messaging network, all communications data between users are routed through WhatsApp servers in accordance with WhatsApp-specific protocols.

Third, the nature of the attack also demonstrates the same. When an insider threat or “inside hacker”—as the Defendants are alleged here to be—seeks to access or misappropriate the “information” of other users in the network—like the messages, files, media, and other information shared on the WhatsApp network and stored on their user devices—it is not an attack on separate individual computer systems, but an attack or trespass on the WhatsApp network itself. Here, the attackers sought access to the WhatsApp network by creating accounts. They then reverse engineered the WhatsApp client and connected it to the network. They then sent malicious code over the network to targeted WhatsApp users, which infected their user devices also via the network. This is because those user devices, loaded with the

94. See Kerr, *supra* note 11, at 1162–63.

95. *Communicating with Others*, ELEC. FRONTIER FOUND. SURVEILLANCE SELF-DEFENSE GUIDE (June 9, 2020), <https://ssd.eff.org/en/module/communicating-others>.

96. See Kerr, *supra* note 11, at 1162.

97. Complaint, *supra* note 23, at 4.

WhatsApp client, are essential for users to interface with the network. From the perspective of the attackers and their target, the boundaries of the WhatsApp network include WhatsApp users and the means by which they interface with the network—individual WhatsApp client accounts on their smartphone devices. Here, while WhatsApp users have separate accounts, they constitute distinct divisions, units, or “areas” within the network but are not separate computer systems. So, the alleged attack did not involve accessing the separate computers of targeted user, with WhatsApp the conduit or staging ground for the attack, but instead involved an accessing information in “other areas” within the WhatsApp messaging network itself—on the accounts of other users.

Lastly, the WhatsApp messaging network clearly falls within the definition of “computers” and “protected computers” in the CFAA.⁹⁸ Again, critics of *WhatsApp v. NSO Group* argue that the proper plaintiffs in the lawsuit should be the targeted users whose smartphones were compromised, not WhatsApp itself.⁹⁹ But these criticisms ignore the fact that these definitions are sweeping in scope and almost certainly cover the WhatsApp messaging network itself, beyond simply its constituent servers and the connected devices of users. Indeed, the broad wording of the “computer” definition includes any “communications facility directly related to or operating in conjunction with” computers like the smartphones and computers used by WhatsApp users.¹⁰⁰ Certainly, the WhatsApp messaging network qualifies as such a “facility” and courts have agreed. The Ninth Circuit in *Nosal (II)* noted that “protected computers” include computer networks, databases, and radio communications networks.¹⁰¹

But beyond the broad definitions, courts have also theorized networks that consisted of individual computers and computerized components under the CFAA as a whole or single system, rather than dividing up the network among those constituent devices or computers for the purposes of analysis. In *Mitra*, for example, the Seventh Circuit upheld the accused’s conviction under the CFAA for intentionally damaging a radio communications network called “SmartNet II,” which was designed by Motorola and used by police,

98. See 18 U.S.C. § 1030(e)(1); see, e.g., *United States v. Nosal (Nosal II)*, 844 F.3d 1024, 1050 (9th Cir. 2016), cert. denied, 138 S. Ct. 314 (2017) (noting “protected computers” include “effectively all computers with Internet access . . . nearly all desktops, laptops, servers, smartphones . . .”).

99. See *supra* note 63.

100. 18 U.S.C. § 1030(e)(1); see *Nosal II*, 844 F.3d at 1050.

101. *Nosal II*, 844 F.3d at 1032 nn.2–3.

fire, ambulance, and other agencies for emergency communication.¹⁰² Justice Easterbrook, writing for the court, found that SmartNet radio communications network was “as a whole” a “protected computer.”¹⁰³ This was despite the fact that the SmartNet had countless computerized constituent elements, including computer hardware and software components, multiple “roaming units,” and a “trunking system” to utilize broadcast frequencies efficiently.¹⁰⁴ This makes sense given the three factors employed above. Ordinary users would certainly perceive SmartNet as best understood as a communications network as a whole, rather than individualized computer components included in the network to ensure it operates properly. The technical realities also support this conclusion, with the various computerized components all included in the network to facilitate core functions of the overall network. Lastly, the nature of the attack also shows supports this conclusion—Mitra did not seek to use the network to hack other computer system, but his aim was to target individual parts of the network in order to disrupt it as a whole. Similarly, the WhatsApp messaging network—and similarly designed internet and social media communications platforms—should likewise be theorized “as a whole,” with different computer components constituting particular areas within the network.

All of these points support the same conclusion—users, and the accounts and devices they use to interface with the WhatsApp network, are best understood as distinct “areas” within the broader computer system itself, the WhatsApp network. And the design of the network means that each user has an individual account tied to a smartphone that cannot be accessed by other users, with end-to-end encryption as a layer of protection to ensure each user’s messages and information are private and not accessible by other users, third parties, or WhatsApp network operators. As such, any existing WhatsApp user that access information in these “other areas”—other user accounts—does so without authorization.

B. CIRCUMVENTING THE CENTRAL CODE-BASED ACCESS BARRIER

As noted earlier, the Defendants had “authorized access” to the WhatsApp network, at least initially.¹⁰⁵ So, the central issue is whether the Defendants *exceeded* that authorized access in carrying out the attack. The meaning of “exceeds authorized access” in the CFAA has been contentious,

102. United States v. Mitra, 405 F.3d 492 (7th Cir. 2005) (recognizing that a radio system is a computer).

103. *Id.* at 494.

104. *Id.* at 493–94.

105. *See supra* note 88 and accompanying text.

but now it is much clearer thanks to *Van Buren*. Now, a user “exceeds” authorized access if they bypass or circumvent an access barrier or gate in order to access or alter information in “other areas” “within a [computer] system” that they never had permission or authorization to access initially.¹⁰⁶ We have already argued that the relevant scope of the computer system in question is the WhatsApp network as a whole, which includes users—who interface with the network via their individual WhatsApp account and WhatsApp clients on their smartphone devices. We have also argued that those user accounts are also distinct “areas” within the network, separated by the general architectural design of the network and end-to-end encryption. As such, on the alleged facts, it is clear that the Defendants in ultimately accessing the “information” in other WhatsApp user accounts—messages, files, data, etc.—and have thus accessed an “other area” within the WhatsApp network. The remaining question, then, is whether a code-based access barrier was bypassed or circumvented in order to access this information.

But as with the scope of the relevant computer system, theorizing the scope and function of the code-based access barrier at issue, and how it was circumvented, also requires subtle legal and theoretical shift. Here, we approach the code-based access barrier—end-to-end encryption—not as simply an authentication gate that the attackers have tricked, compromised, or otherwise passed through. Rather, we focus on how the attackers circumvented a broader intended function in the WhatsApp network—protecting the privacy and security of communications and other information shared on the network.

1. *The Access Circumvented a Code-Based Access Barrier*

The Defendants’ alleged hack here violated a clear and express “code-based” prohibition on access built into the WhatsApp messaging network end-to-end encryption.¹⁰⁷ Code-based limitations are attempts to enforce an owner’s intent to limit authorization through the use of software, hardware, or other technical related measures.¹⁰⁸ Such restrictions are important because they define not only the limits of access but also communicate the owner’s intent to limit access.¹⁰⁹ End-to-end encryption plays this role in WhatsApp. This code-based restriction or prohibition is “express[ed]” both as a feature highlighted and communicated by WhatsApp, but also in the architecture

106. KOSSEFF, *supra* note 7, at 176–80; Mayer, *supra* note 17, at 1657–58.

107. Goldfoot & Bamzai, *supra* note 11, at 1487; *see* Kerr, *supra* note 11, at 1147.

108. Goldfoot & Bamzai, *supra* note 11, at 1487.

109. *Id.* at 1490.

itself. In fact, it is a central technical WhatsApp feature, ensuring messages sent by users are protected by an end-to-end encryption protocol—where each message is encrypted with both a public and private key before being sent so that only the recipient can decrypt and read the messages. This is all apparent in Figure 2, discussed earlier.

But it is not just messages that are encrypted in this network. Rather, the entire communications network is protected in a layer of end-to-end encryption. Meaning every step and function in the network—from messaging session initiation, to receiving session setup, to messaging exchange, to transmitting media and other attachments, to group messages, to voice and video call setup, to status and location updates—is protected by end-to-end encryption.¹¹⁰ Thus, if a third party could intercept a message before it arrived with the recipient, they would not be able to decrypt without the recipient’s private key. This code-based restriction, which protects the privacy and security of all WhatsApp user messages, applies both to insiders and outsiders. That is, the encryption ensures only the intended recipient can decrypt and read messages—not other users, nor hackers or attackers outside the network, nor even WhatsApp itself.¹¹¹ As earlier noted, encryption has long been recognized as a “code-based” restriction on access under the CFAA.¹¹² The difference here is that it is not a single file or transfer that is encrypted to prevent access; rather, the entire WhatsApp messaging network is enclosed by end-to-end encryption—a clear and express prohibition on access to communications within the network.

2. *The Attackers Knew of the Code-Based Access Barrier*

The Defendants, on these alleged facts, knew of the code-based restriction—the end-to-end encryption. Beyond being a central technical and architectural feature of WhatsApp’s messaging network, encryption is highlighted and persistently advertised on the WhatsApp website as a key feature, including in a technical white paper available on the site.¹¹³ In fact, the entire hack, visualized in Figure 3, evinces a sophisticated understanding of the WhatsApp network and its encryption protocol.

110. See WHATSAPP ENCRYPTION, *supra* note 80, at 11.

111. See *id.*

112. See Kerr, *supra* note 21, at 1666 (analyzing a scenario involving an encrypted internet connection as a “code-based” restriction under the CFAA); see also Clark S. Splichal, *Recent Development: Craigslist and the CFAA: The Untold Story*, 67 FLA. L. REV. 1845, 1856 (2015) (noting encryption is a “conventional” technological or code-based “barrier” like passwords).

113. See WHATSAPP WEBSITE, *supra* note 80; *WhatsApp Security*, *supra* note 80; *WhatsApp Faq*, *supra* note 80; WHATSAPP ENCRYPTION, *supra* note 80.

Figure 3: The Alleged WhatsApp Messaging Network Hack—Multiple steps and involving multiple provides unauthorized access and exploitation of every aspect of WhatsApp’s messaging network.

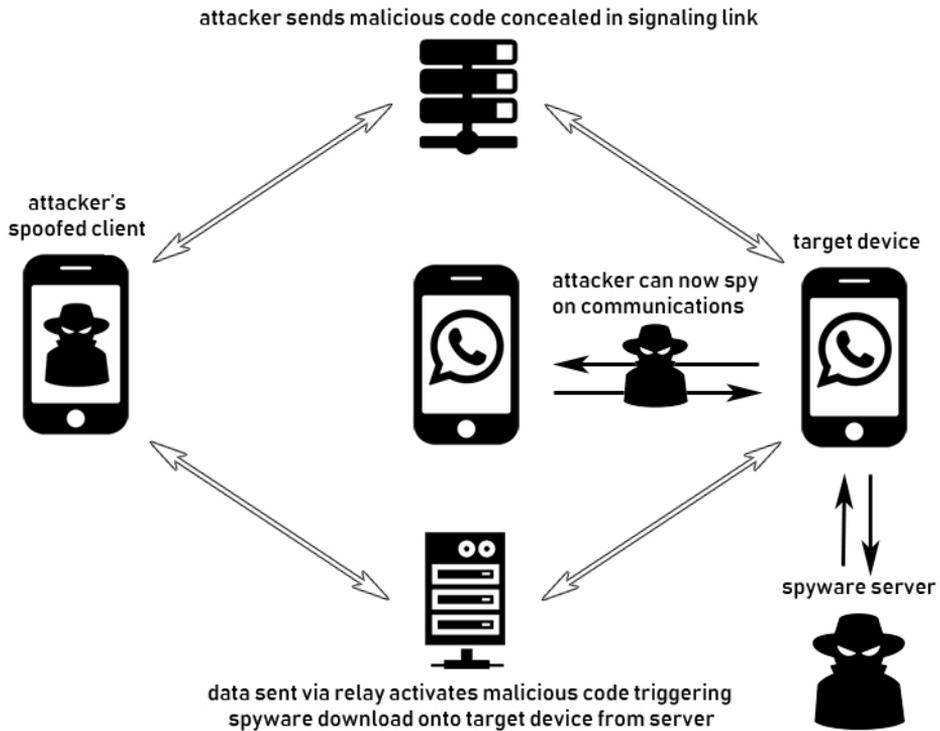


Figure 3 helps illustrate that instead of attempting to break the encryption from the outside, the attackers focused on circumventing it by targeting vulnerable points in the WhatsApp messaging network—WhatsApp clients, network protocols, server nodes, and target devices—to get around the encryption protection and obtain unauthorized access to communications within the network. The Defendants, the Complaint alleges, first created “various WhatsApp accounts” and then “reverse-engineered” the WhatsApp user app in order to develop a spoofed WhatsApp client program (“spoofed client” in Figure 3).¹¹⁴ This spoofed WhatsApp client was able to emulate “legitimate” WhatsApp messaging network traffic, thus enabling them to send “malicious code”—undetected—via the WhatsApp messaging network.¹¹⁵ The Defendants then transmitted malicious code via the

114. Complaint, *supra* note 23, at 7–8.

115. Complaint, *supra* note 23, at 8.

WhatsApp messaging network, specifically the Signaling Servers, to the targeted user (“target device” in Figure 3).¹¹⁶ This instance of malicious code—which could be delivered simply by a missed WhatsApp call on the target device—was specially designed to exploit a flaw in WhatsApp’s end-to-end encryption protocol, allowing it to install in the memory of the target device.¹¹⁷ An additional instance of malicious code was then transmitted by the Defendants, this time via the WhatsApp Relay Servers, which triggered the download of spyware onto the target device from a remote server controlled by the Defendants.¹¹⁸ The spyware, once installed, could be controlled remotely by the Defendants and provided them access to all data on the target device, including access to WhatsApp messages, call logs, and other data and information shared on the WhatsApp network that was previously inaccessible because of encryption.¹¹⁹ The alleged spyware in question—Pegasus—is specifically designed to circumvent end-to-end encrypted communications on services like WhatsApp, as once it is downloaded and installed on a target device, it is designed to intercept messages before they are encrypted on the client application and sent across the network or after the client applications decrypts.¹²⁰

The Defendants carried a multi-step sophisticated hack, specifically designed to exploit unique aspects and vulnerabilities in the WhatsApp messaging network to circumvent a central code-based restriction built into the WhatsApp messaging network as a whole: end-to-end encryption protection for user messages. Like the hack in *Barrington* found to violate the CFAA, this hacking scheme also involved “multiple, repetitive and coordinated steps to deceive and exploit” WhatsApp’s encryption-protected network.¹²¹ Also like *Barrington*, it involved “repetitive and coordinated activities by numerous individuals” who used “sophisticated technology” to carry out and “conceal” the scheme.¹²² This kind of sophisticated attack that

116. Complaint, *supra* note 23, at 8.

117. Checkpoint Research, *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

118. Checkpoint Research, *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48; Complaint, *supra* note 23, at 7.

119. *See* Checkpoint Research, *supra* note 49; Srivastava, *supra* note 48; Wong, *supra* note 48.

120. *See* Complaint, *supra* note 23, at 6; Lorenzo Franchesci-Bicchierai & Joseph Cox, *The DEA Didn't Buy Malware From Israel's Controversial NSO Group Because It Was Too Expensive*, VICE: MOTHERBOARD (Sept. 11, 2019), https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo; *Protecting our users from a video calling cyber attack*, WHATSAPP (Oct. 29, 2019), <https://faq.whatsapp.com/general/security-and-privacy/protecting-our-users-from-a-video-calling-cyber-attack/?lang=en> (explaining the NSO Group’s attack).

121. *United States v. Barrington*, 648 F.3d 1178, 1199 (11th Cir. 2011).

122. *Id.*

led to access and entry to user devices is precisely the kind of malicious activities the CFAA should deter and police.

Indeed, the visualizations in Figures 2 and 3 also help illustrate how WhatsApp messaging service operates like a system or network enclosed by encryption protection from end-to-end, and how the attack was an attack or unauthorized trespass on that network as a whole. And this encryption, which encloses the network, defines unauthorized access and any access that exceeds authorized access. In this sense, it was like the attack on the radio communications network in *Mitra*, which compromised the integrity and operations of the network. WhatsApp is not just users messaging across the internet; it is a sophisticated messaging network with nodes, servers, and users—like a circuit—and protected by encryption throughout. The Defendants exploited multiple vulnerabilities in various parts of the network—Signaling Servers, Relay Servers, user client apps, and user devices, among others—to go around it and target the weaker end-points—the unencrypted user devices.

If this theory and the facts underlying it are proven at trial, assuming the case proceeds that far, they will support multiple CFAA claims. They clearly demonstrate not only that the Defendants knew about the end-to-end encryption in the WhatsApp messaging network but intentionally circumvented it to access information in “other areas” in the “computer system”—the messages, files, media, and shared information of other WhatsApp users—to which their initial authorized access did not entitle them to access.¹²³ This was “information” they were not entitled to access and which was “in the computer,” that is, in the WhatsApp network itself. As such, the Defendants would have “exceeded authorized access” to the WhatsApp messaging network contrary to section 1030(a)(2)(C).¹²⁴ On the CFAA’s broad definitions of “damage,” this will have certainly “damaged” the network by impairing its integrity.¹²⁵ These actions would almost certainly caused a “loss” to one or more persons (sections 1030(e)(11) and 1030(c)(4)(A)(i)(I)) and caused “damage” by impairing the integrity of the WhatsApp network (section 1030(e)(8)) by undermining its end-to-end encryption protections.

123. 18 U.S.C. § 1030(a)(2)(C); *id.* § 1030(e)(6).

124. 18 U.S.C. § 1030(a)(2)(C); *id.* § 1030(e)(6).

125. 18 U.S.C. § 1030(e)(8) (“[T]he term ‘damage’ means ‘any impairment to the integrity or availability of data, a program, a system, or information.’”); *id.* § 1030(e)(6).

V. A NETWORK TRESPASS THEORY OF LIABILITY

We have argued that the alleged attack on WhatsApp’s encrypted messaging network is best understood using what we call a network trespass theory of liability. This theory holds that accessing a network and using it to hack or stage an attack on users of that network—like obtaining unauthorized access to their personal computing devices by circumventing end-to-end encryption—should be treated as trespass not just on the individual devices of the targeted users, but on the network itself, and it should thus attract liability under the CFAA.

The theory is consistent with the narrow reading of the CFAA endorsed in *Van Buren* and, applied to the alleged facts of *WhatsApp v. NSO Group*, offers a full answer to criticisms. Critics argued that the *WhatsApp* lawsuit relies too heavily on breach of the terms of service as a foundation for its claims under the CFAA.¹²⁶ And, to be clear, the Complaint does cite WhatsApp’s Terms of Service and alleges that the Defendants accepted those terms.¹²⁷ Our network trespass theory of liability, however, focuses on how the Defendants circumvented code-based restrictions, avoids the problems critics raise, and is entirely consistent with a narrow interpretation of the CFAA, endorsed by the Supreme Court in *Van Buren*. To be clear, our network trespass theory does offer a new and novel approach to theorizing the “boundaries” of the “relevant computer system” and the “information and services with that system” in the CFAA analysis.¹²⁸ But this, as we have argued, is a better legal, theoretical, and technical understanding of the WhatsApp network.

A. THE CFAA’S POLICY AIMS

Why should this theory be applied here and beyond? First, imposing liability here, based on our network trespass theory, would advance the underlying policy aims of the CFAA. The statute was enacted in response to concerns about the growing threat hackers posed to computers and their security, both insiders and outsiders.¹²⁹ The sophisticated multi-stage hack carried out on the WhatsApp messaging network—to circumvent its end-to-end encryption protection of user communications—is precisely the kind of hack the CFAA was intended to cover. When applying the “intended function test” from the famous *Morris* worm case, for instance, the

126. See Ekeland, *supra* note 31; Greenberg, *supra* note 33 (quoting Ekeland and Pfefferkor); Condliffe, *supra* note 30 (quoting Ekeland and Pfefferkor).

127. Complaint, *supra* note 23, at 4, 7.

128. Mayer, *supra* note 17, at 1646.

129. Winn, *supra* note 73, at 1402–03; Goldfoot & Bamzai, *supra* note 11, at 1481–82.

allegations show the Defendants clearly did not use the WhatsApp network as intended: not for messaging, but to circumvent encryption in order to access the messages of other users without authorization.¹³⁰

Additionally, the statute, when passed, aimed not only to protect the security and integrity of computers and computer networks from hackers and unauthorized intrusion—hence the incorporation of legal concepts from trespass law—but also to protect information and data contained on computers.¹³¹ Encryption is an essential technological tool for such protection. Today, it is considered a “fundamental architectural safeguard” that permeates both law and private-sector cybersecurity frameworks.¹³² And for the Financial Industry Regulatory Authority (FINRA), encryption is a “critically important” tool in a firm’s cybersecurity “arsenal.”¹³³ Thus, as a long-recognized “code-base” restriction on access that is now also “essential” to ensuring security and privacy in new forms of electronic communications systems,¹³⁴ imposing liability here is fully consistent with the CFAA’s aims.

B. BETTER PRIVACY AND SECURITY OUTCOMES

Though the original CFAA statute did not highlight privacy concerns, subsequent amendments, particularly in 1996, made privacy concerns clear.¹³⁵ Concerns about protecting privacy in information to restore public faith in computer security can be found throughout legislative debates about the amendments.¹³⁶ Pursuant to these aims, enforcement and liability here would also lead to better privacy and security outcomes in the long term.

First, it offers an additional legal lever to deter and police insider threats under the CFAA. Cybercriminals, hackers, and other malicious actors have long used the computers, networks, and servers of others as staging grounds, mediums, or intermediaries to carry out attacks, hacking, and other illegal and

130. See *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991); Kerr, *supra* note 21, at 1631–32.

131. Winn, *supra* note 73, at 1404; Goldfoot & Bamzai, *supra* note 11, at 1481–82.

132. William McGeeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1175 (2019).

133. *Id.* at 1190.

134. Tole Sutikno, Lina Handayani, Deris Stiawan, Munawar Agus Riyadi & Imam Much Ibnu Subroto, *Whats.App, viber and telegram: Which is the best for instant messaging?*, 6 INT’L J. ELECTRICAL & COMPUTER ENGINEERING 909, 911 (2016).

135. Winn, *supra* note 73, at 1404–05; Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 330–31 (2004).

136. See Winn, *supra* note 73, at 1404–05; see also Galbraith, *supra* note 135, at 330–31.

disruptive activities online.¹³⁷ Such cases have raised the issue, also long debated, as to how the law should deal with intermediaries whose platforms are used and abused by hackers and malicious actors for such illicit activities,¹³⁸ including what recourse or protections such intermediaries might have under CFAA.¹³⁹ This issue has taken on even greater urgency in a world where popular social media and communications platforms—like Facebook, Twitter, and WhatsApp—are now ubiquitous, as these platforms typically

137. In fact, one of the first hacking cases prosecuted under the CFAA was the *Morris* case. See *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991). Edward Morris, then a Cornell graduate student, was prosecuted for damage caused by his computer worm, which infected computers and spread around the world via the internet. To launch his worm, Morris hacked into a computer at Massachusetts Institute of Technology (MIT) to conceal its origins. It did not work. See *The Morris Worm*, FBI NEWS STORY (Nov. 2, 2018), <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>; see also Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, 11–14 (2002) (detailing the story of “Mafiaboy,” a 15-year-old “script kiddie” living with his parents in a Montreal suburb, who took down several major websites in February 2000 with a distributed denial of service (DDoS) attack, which often made possible by a network of infected third party intermediaries or “zombie” computers and servers); Helen Nissenbaum, *Where Computer Security Meets National Security*, in CYBERCRIME DIGITAL COPS IN A NETWORKED ENVIRONMENT 63 (Jack Balkin, James Grimmelman, Eddan Katz, Nimrod Kozlovski, Shlomit Wagman & Tal Zarsky eds., 2006) (noting use of networked computers as staging grounds or mediums for online attacks and other disruptive activities as a key category of cybersecurity threats).

138. See, e.g., Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 29, 53–54 (2000) (arguing for nuisance law principles to apply in the internet context); Adam Mossoff, *Spam-Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625, 647–48 (2004) (similar); Henderson & Yarbrough, *supra* note 137, at 16–18 (exploring both the duty and standard of care, on a negligence law standard, involved in protecting a person’s own computer against becoming a staging ground for attacks); T. Luis de Guzman, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 551–54 (2010) (arguing owners of infected computers in “botnet” or “zombie” networks—often used in DDoS and similar attacks—should be held liable to DDoS victims under a negligence theory).

139. See, e.g., Laura Bernescu, *When is a Hack not a Hack: Addressing the CFAA’s Applicability to the Internet Service Context*, 2013 U. CHI. LEGAL F. 633 (2013) (considering CFAA’s application to online service providers); see generally Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 168–74 (2018) (analyzing the CFAA’s application to the Internet of Things and similar common intermediaries for forms of online attacks); Shane Huang, *Proposing a Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229 (2014) (arguing that existing legal options are insufficient and proposing that the CFAA be amended to allow for innocent intermediaries of hacking and other cybercrimes to “hack back,” that is, hack into the computer systems and servers of perpetrators and other third parties to deter attacks or assist in attribution); Chris Cook, *Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook*, 29 STAN. L. & POL’Y REV. 205 (2018).

have hundreds of millions, even billions, of users—a target rich environment for malicious actors—and are generally accessible to anyone with an internet connection.¹⁴⁰ This has created a range of new “insider” threats and risks, as users that already have authorized access to a platform or network—hence an insider—can use that access to target other users, misappropriate data and information, or carry out attacks or other illicit activities against targets elsewhere online.¹⁴¹

However, the Supreme Court in *Van Buren*, as earlier noted, significantly narrowed CFAA scope in deterring and policing such insider threats by finding there is no criminal or civil liability under the CFAA for improper use of that system or information—like using a platform as a staging ground to hack, target users, or engage in other illegal activities. Now, the only way an insider threat can exceed their authorized access under the CFAA is when they access files, data, or information in other areas “in the computer” to which they had no access to begin with.¹⁴² Our approach offers a new theory of network trespass liability to allow platforms and networks like WhatsApp to legally defend themselves from insider threats.

Indeed, applying CFAA restrictions to prohibit and punish this sophisticated hack would help deter hackers and other bad actors—such as firms creating, selling, and distributing spyware and malware—from similarly attacking and circumventing similar encryption protocols in the future. Indeed, it has been recently argued that a negative consequence of the WhatsApp lawsuit, if such lawsuits become more common, is it may cause the “market in cyber vulnerabilities” to “dry up,” limiting the government’s capacity for legal hacking as there would be fewer “cyber vulnerabilities” for it to purchase or acquire from private actors.¹⁴³ Having fewer cyber vulnerabilities being bought, traded, and shared would be a positive outcome for privacy, security, and human rights in the long run. As Justice Fletcher wrote in *Bernstein v. United States*, the availability and use of encryption by citizens offers the opportunity to “reclaim some portion of the privacy we have lost” through increasing electronic communications.¹⁴⁴ By providing protection for encryption protocols in messaging networks like those WhatsApp employed and in deterring exploitation of those systems, the CFAA can help promote such privacy aims.

140. See Margetts, *supra* note 15, at 107–08.

141. See *supra* note 15; WRIGHT, *supra* note 14, at 40. As mentioned, “insiders” commit most cybercrime. See Mayer, *supra* note 14, at 1493.

142. 18 U.S.C. § 1030(e)(6).

143. Rozenshtein, *supra* note 40; McGeeveran, *supra* note 132, at 1191.

144. *Bernstein v. United States*, 176 F.3d 1132, 1146 (9th Cir. 1999).

It would also, in turn, encourage more companies and social media platforms to employ end-to-end encryption to ensure the privacy and security of users. Privacy law scholar William McGeeveran, for instance, recently argued for a “duty of data security” that includes a mandatory duty to use encryption in certain circumstances.¹⁴⁵ One such instance might include services or platforms comparable to WhatsApp where data is constantly “in transit”—like being transmitted between servers or users on a messaging network.¹⁴⁶ Beyond the technical safeguards encryption provides, the law could also provide an additional remedy when encryption is attacked, hacked, circumvented, or broken through sophisticated security vulnerability exploits or malicious code and programs designed to extensively invade the privacy of targeted users.

However, beyond outsider threats and attackers, it may be argued that this approach creates liability risks for existing users—network insiders—who use platforms like Facebook or WhatsApp contrary to how they were intended, like using “knock off” versions of smartphone applications.¹⁴⁷ These concerns are misplaced. First, on our network trespass theory, such activities—like using a knock off version of WhatsApp on the WhatsApp network—would not “exceed authorized access” as they would not involve circumventing a code-based restriction to access “information”—encrypted communications—of other user accounts on the system, as the Defendants have done here. Again, to attract liability for “exceeding” authorized access on a narrow interpretation of the CFAA involves circumventing code-based restrictions on access to services or information within the system that the user did not have access to initially. A “knock off” app that is only restricted by TOS and not any code-based or technological barrier would not attract liability. Second, these concerns also ignore *mens rea*, or intentions, a “critical” component of CFAA analysis.¹⁴⁸ The CFAA was enacted to address “serious computer break-ins,”¹⁴⁹ and such activities on the network simply do not qualify. If, however, creators of a knock-off app did so with the intent to exploit vulnerabilities in a network to surreptitiously access encrypted communications of other users—and did so—then this would be an *intent* and *conduct* that could lead to CFAA. Users taking advantage of “knock off”

145. McGeeveran, *supra* note 132, at 1190.

146. McGeeveran, *supra* note 132, at 1191.

147. See Yomi Kazeem, *WhatsApp is so popular in Africa, even knock-off versions are used more often than Facebook*, QUARTZ AFRICA (Mar. 5, 2020), <https://qz.com/africa/1804859/fake-whatsapp-app-more-popular-than-facebook-instagram-in-africa/>.

148. See Kerr, *supra* note 11, at 1180.

149. Jamie Williams, *Automation Is Not “Hacking”: Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 B.U. J. SCI. & TECH. 416, 437–41 (2018).

apps with different basic features to communicate legitimately with other users would not. By contrast, the Defendants alleged attack on the WhatsApp network, which circumvented encryption barriers, is clearly an intentional and “serious computer break-in”¹⁵⁰ in terms of the network.

C. CORPORATE ACCOUNTABILITY FOR HUMAN RIGHTS VIOLATIONS

There is a broader international human rights context to the WhatsApp lawsuit, providing a good reason to support it beyond the legal or technical aspects of its claims. Though the lawsuit only asserts claims under U.S. laws like the CFAA, its international dimensions are clear. For instance, the Citizen Lab, as earlier noted, identified at least one hundred cases of human rights defenders victimized by the attack globally, including activists, dissidents, lawyers, and journalists throughout the world.¹⁵¹ And WhatsApp CEO Will Cathcart cited privacy as a “fundamental right” and argued, “technology companies must deepen our cooperation to protect and promote human rights.”¹⁵²

But the human rights concerns raised by transnational private sector technology companies like NSO Group go far beyond one single company. The Citizen Lab, for example, has documented numerous instances of private sector companies operating internationally and contributing to human rights abuses.¹⁵³ Filtering technology developed by Canadian company Netsweeper, for instance, has been used by governments with poor human rights records around the world to censor digital speech, including content concerning human rights, health, and religious minorities.¹⁵⁴ A range of other technology and cybersecurity firms like Germany-based FinFisher, Italy-based Hacking Team, and the U.S.-based company Sandvine develop spyware and malware that has likewise been used by governments globally to track human rights activists, journalists, and dissidents.¹⁵⁵ Thus, in explaining its lawsuit, WhatsApp cited the Citizen Lab’s work as well as UN Special Rapporteur for Freedom of Expression David Kaye, who called for a moratorium on spyware-enabled “attacks.”¹⁵⁶ The post also cited Amnesty

150. *See id.*

151. CITIZEN LAB, *supra* note 54.

152. Cathcart, *supra* note 25.

153. *See* Jonathon Penney, Sarah McKune, Lex Gill & Ronald J. Deibert, *Advancing Human Rights in the Dual Use Technology Industry*, 71 COLUM. J. INT’L AFF. 103, 105–07 (2018); *see generally* Anna W. Chan, *The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware*, 44 BROOK. J. INT’L L. 795 (2019).

154. Penney, *supra* note 153, at 103; Chan, *supra* note 153, at 795–97.

155. *See* Penney, *supra* note 153, at 105; Chan, note 153, at 801.

156. WHATSAPP, *supra* note 120.

International's work and called for "strong legal oversight of cyber weapons like the one used in this attack" to ensure they are not used to violate the rights and freedoms of people "wherever they are in the world."¹⁵⁷

The challenge, of course, is that presently there is almost no legal oversight for spyware, malware, censoring tools, and other forms of "cyber weapons" developed, marketed, sold, and distributed globally by transnational technology companies. Though many of the uses of these tools and technologies directly implicate international human rights law—including provisions in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights¹⁵⁸—there is no clear avenue where these human rights abuses can be enforced nationally or internationally. International law, for instance, primarily imposes legal obligations on states and state actors, not non-state actors like these companies, thus leaving clear regulatory gaps.¹⁵⁹ And there is no effective international mechanism to hold these companies accountable for human rights abuses.¹⁶⁰ Furthermore, "soft" international law like the UN Guiding Principles on Business and Human Rights, while helpful, remains largely voluntary and provides no new means of accountability.¹⁶¹ Finally, remedies under domestic law for international victims have also proven largely inadequate.¹⁶² Domestic courts regularly decline jurisdiction, for instance, citing more appropriate venues elsewhere.¹⁶³ Though for a time the U.S. Alien Tort Statute provided hope for recourse in American courts, recent Supreme Court decisions have severely limited its scope and application.¹⁶⁴ Finally, the legal basis for states to regulate the extraterritorial activities of businesses is also murky, with international human rights law offering little guidance.¹⁶⁵

In short, there is a large accountability gap when it comes to technology companies operating internationally and contributing to human rights abuses.¹⁶⁶ The *WhatsApp* lawsuit offers a possible path forward for greater

157. *Id.*

158. Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473, 475–82 (2016); Chan, *supra* note 153, at 802–05.

159. Chan, *supra* note 153, at 805–13; Penney, *supra* note 153, at 104–05.

160. Chan, *supra* note 153, at 806–07; Penney, *supra* note 153, at 104–05.

161. Chan, *supra* note 153, at 809–10.

162. Chan, *supra* note 153, at 811–13; Penney, *supra* note 153, at 104–05.

163. Chan, *supra* note 153, at 811–12.

164. *Id.*; Jonathon Penney, *The Cycles of Global Telecommunication Censorship and Surveillance*, 36 U. PA. J. INT'L L. 693, 742–43 (2015).

165. Penney, *supra* note 153, at 105.

166. Chan, *supra* note 153, at 818–19 (suggesting they have "a bubble of impunity").

accountability: private sector legal action on behalf of users and victims abroad. Rather than only the targeted victims of abuses having a responsibility to take legal action for remedies and redress, *WhatsApp v. NSO Group* stands as an example of private sector action that advances human rights interests through greater accountability for corporate abuses, not just in the United States, but internationally as well. Though taking us into “uncharted” legal territory,¹⁶⁷ if successful, it may lay the foundation of new possibilities for corporate accountability, beyond mere public shaming via media coverage. This is another good reason to defend the lawsuit.

D. IMPLICATIONS: *VAN BUREN* AND BEYOND

1. *Taking the Scope of the Computer System or Service Seriously*

There are other implications of our analysis. One is that courts and scholars need to take more seriously the task of theorizing the scope and boundaries of the relevant computer system, service, and the information accessed or obtained. As noted earlier, this has always been an important though neglected issue under the CFAA analysis—you have to define the targeted computer and its scope to determine if someone has accessed it without authorization or exceeded authorizing if already accessing it. After *Van Buren*, the question has arguably become even more important, but also more complex, especially when dealing with attackers with access to the computer system. This is because the Supreme Court’s reasoning suggests it favors a code-based approach to access barriers and gates, which means that determining liability depends even more on the contours and nuances of the system or network in question. Now, one needs to understand not just the boundaries of the relevant computer system, but also the different “areas” within it, as a user with authorized access exceeds it only if they bypass an access barrier or gate and reach “other areas” within that system to which their authorized access does not extend.¹⁶⁸

Yet, this is an issue that courts have often not addressed adequately.¹⁶⁹ In *United States v. Phillips*,¹⁷⁰ for example, the Fifth Circuit found that a University of Texas student accessed a course management website without authorization when he guessed passwords to various faculty and staff

167. Newsroom, *supra* note 32.

168. Atlas et al., *supra* note 10; Cunningham, Grant & Hoofnagle, *supra* note 19.

169. Mayer, *supra* note 17, at 1651–53 (noting that “courts have not seriously defined the scope of a computer system...”); Kerr, *supra* note 21, at 1653 (noting the *Morris* case “raised questions about how to divide a network of computers into individual computers for the purpose of the statute,” though those issues were ignored by the Second Circuit on appeal).

170. *United States v. Phillips*, 477 F.3d 215 (5th Cir. 2007).

accounts on the system.¹⁷¹ However, the court failed to address the specific computer system that was accessed without authorization.¹⁷² Was it the course website itself? Each individual account the student accessed? Or the database accessed via the course website? This is important as depending on the answer the magnitude of the hack and the number of “computer systems” accessed without authorization could be substantially different (one website accessed versus multiple user accounts accessed). However, the court did not address the matter.¹⁷³ The famous *Morris* case, one of the earliest significant CFAA cases, also involved a similar issue. In that case, Edward Morris, then a Cornell graduate student, was prosecuted for damage caused by his computer worm, which infected computers and spread around the world via the internet.¹⁷⁴ To launch his worm, Morris hacked into a computer at Massachusetts Institute of Technology to conceal its origins.¹⁷⁵ On appeal, a key issue was theorizing and defining the “computer system” at stake. Did Morris engage in a single act of access when he sent his worm over the internet, or was he responsible for every computer that his worm infected thereafter? Also, should the internet, a single network, be divided into individual computers for the purposes of CFAA liability? Unfortunately, again, the Second Circuit did not directly address the issue.¹⁷⁶ After *Van Buren*, both courts and scholars need to take this issue more seriously.

To that end, we have set out a framework for helping determining the scope of the relevant computer system or service and the information therein for CFAA purposes. This “objective” approach takes into account the perceptions of ordinary users; the technical realities of the computer system, service, and information; and the nature of the hack itself. It asks: what was the information the attackers were targeting and what was their methodology? This approach illuminated the proper scope and boundaries of the WhatsApp network, and, looking back, also explains the court’s reasoning in the *Mitra* case and how the court treated that network as a whole. We believe it likewise can help arrive at better liability determinations under the CFAA going forward, especially in a post-*Van Buren* world.

171. *Id.* at 219–21.

172. *Id.* at 219–21; Mayer, *supra* note 17, at 1652.

173. *Phillips*, 477 F.3d at 218; Mayer, *supra* note 17, at 1652.

174. *United States v. Morris*, 928 F.2d 504, 505–04 (2d Cir. 1991).

175. *See* FBI NEWS STORY, *supra* note 136 (noting Morris hacked into an MIT computer to launch his computer worm).

176. *See* Kerr, *supra* note 21, at 1631, 1631 nn.147–53.

2. *Theorizing and Defining Access Barrier Circumvention*

Another implication is that scholars and courts should take more seriously the task of defining or theorizing what it means to circumvent a code-based access barrier, which has also become increasingly important after *Van Buren*'s narrow construction of the CFAA. Scholars and courts have been prolific in formulating different approaches to "authorized access" under the CFAA, but few have focused systematically on how to theorize different code-based barriers nor parsed what bypassing or circumventing such a barrier requires. Leading scholars like Orin Kerr have argued that the best way to approach code-based access restrictions is as authentication gates, that is, technological measures that require verifying that the user is the person who has access rights to the information accessed,¹⁷⁷ like a portal requiring a password to allow access. This approach has begun to gain traction among courts as well. The U.S. District Court's recent decision in *Sandvig v Barr*¹⁷⁸ held, citing Kerr, that CFAA liability was only triggered only when a defendant bypassed an authentication gate.¹⁷⁹ And there are passages in *Van Buren* suggesting the Supreme Court also favors this approach.¹⁸⁰

The challenge is that theorizing code-based access barriers only as authentication gates may lead courts to define bypassing or circumvention too narrowly. This is apparent from Kerr's original test for circumvention, which he defined as "tricking the computer" into giving the user "greater privileges" when "computer code" has been used "to create a barrier designed to block the user from exceeding his privileges on the network."¹⁸¹ This more narrow inquiry neglects how attackers can formulate sophisticated attacks that entirely ignore the authentication function of the code-based barrier and instead wholly circumvent or "workaround" it, rather than tricking the authentication gate into allowing access or exploiting a

177. Kerr, *supra* note 11, at 1146; Kerr, *supra* note 21.

178. *Sandvig v. Barr*, No. CV 16-1368, 2020 WL 1494065 (D.D.C. filed May 28, 2020), <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/06/Sandvig-v-Barr.pdf>.

179. *Id.*

180. *Van Buren v. United States*, 141 S. Ct. 1648, 1659 n.9 (2021). The Court here cites *Bellia*. *Id.* But *Bellia* on the page cited by the court actually cites Kerr for the definition of authorization as authentication. *See Bellia*, *supra* note 69, at 1470 nn.158–59.

181. Kerr, *supra* note 11, at 1146 (both discussing and quoting Kerr, *supra* note 21, at 1644–46). In fairness to Professor Kerr, he later changed this definition to focus on authentication. *See* Kerr, *supra* note 11, at 1146. But even that definition may not work as, here, access arguably did not fall "outside authentication" since the user devices provided authentication; it just happened they were controlled by the attackers. A better way to understand the attack methodology, in our view, is that it aimed to obtain user data and communications by avoiding circumventing the end-to-end encryption on the network itself.

vulnerability in the gate that gives the attacker greater privileges.¹⁸² One example of such a workaround is to attack the weaker “end points” in the network—like the devices of users—where plaintext versions of unencrypted communications can be obtained.¹⁸³ This is especially the case with stronger forms of code-based access barriers—like encryption—that are very hard to trick, compromise, or break.¹⁸⁴ Rather, attackers typically seek to work around the encryption, and that is what the attackers did in *WhatsApp v. NSO Group*. But this particular attack likely would not fall into Kerr’s definition. Under his test, it would seem the attackers have not circumvented anything—no trickery to fool authentication, credential misappropriation, or hack to pass through the code-based barrier. They have simply carried out a sophisticated “encryption workaround.”¹⁸⁵ But this, too, should trigger CFAA liability.

In fairness, Kerr has offered a newer test focused on authentication that is stronger but may also have problems with “work around” attacks. Kerr says the “key point is not that some code was circumvented” but that “the computer owner conditioned access on authentication of the user and the access was outside the authentication.”¹⁸⁶ This test was likewise adopted by the court in *Sandvig*.¹⁸⁷ But was access here “outside authentication”? In one sense, yes, in that attackers did not have the cryptographic key to decipher encrypted WhatsApp messages and still gained access. But in a technical sense no, in that messages and other information obtained on the user devices were in plain text; the user had the right credentials for authentication, just the attackers used malicious code to take control of the user’s device to avoid dealing with encryption restrictions at all.

One way to avoid these problems is, as we have done in our analysis, to consider the *intended function* of code-based barrier or authentication gate in determining if an attacker has “circumvented” the barrier access or whether access is “outside authentication,” to use Kerr’s terms, to trigger liability. The “intended function test” was first set out in the famous *Morris* worm case,¹⁸⁸

182. Kerr & Schneier, *supra* note 1; Clarke & Ali, *supra* note 3; Squire, *supra* note 8.

183. Kerr & Schneier, *supra* note 1, at 1007–10.

184. Kerr & Schneier, *supra* note 1, at 1006–07; Clarke & Ali, *supra* note 3; Squire, *supra* note 8.

185. Kerr & Schneier, *supra* note 1.

186. Kerr, *supra* note 11, at 1164.

187. *Sandvig v. Barr*, No. CV 16-1368, 2020 WL 1494065 (D.D.C. filed May 28, 2020), <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/06/Sandvig-v-Barr.pdf>.

188. *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991); Kerr, *supra* note 21, at 1631–32.

wherein Edward Morris exploited vulnerabilities in multiple programs, like the SENDMAIL emailing program, that gave him unintended access to areas and information on the system.¹⁸⁹ The court held that he did not use these programs “in any way related to their intended function.”¹⁹⁰ We are transplanting this test to a slightly different part of the CFAA analysis—not to understand when access is not authorized, but to understand the nature of code-based barriers and their functions to better understand methods to circumvent them. Indeed, code-based limitations are attempts to enforce an owner’s intent to limit authorization through the use of software, hardware, or other technical related measures.¹⁹¹ Such barriers define not only the limits of access but also communicate the owner’s intent to limit access.¹⁹² Thus, we would slightly modify Kerr’s test for authentication or circumvention, where liability is triggered when “access is outside authentication or *inconsistent with the intended function of the authentication.*” Applying this here shows that the attackers accessed information on user devices *inconsistent with its intended function* of end-to-end encryption in the WhatsApp network, which was to protect the privacy and security of WhatsApp user communications from all third parties, including other users in the network. The access was inconsistent with that intended function.

VI. CONCLUSION

In our view, the critical reception to the *WhatsApp* lawsuit—and the CFAA violations it claims—is not justified. If based on our network trespass theory, we believe there is a sound basis for CFAA claims. The *WhatsApp v. NSO Group* case has the potential to improve corporate accountability for human rights. Our analysis can also lead to better privacy and security outcomes and provides guidance on critical post-*Van Buren* issues. First, our analysis theorizes sophisticated code-based access barriers and their circumvention under the CFAA, including how the law is best applied to encrypted messaging networks and similar social media platforms. Second, it theorizes the scope, boundaries, and areas of the relevant computer system, services, and information therein to determine CFAA liability. These issues have long been neglected by both courts and scholars, but after *Van Buren* that neglect cannot be sustained.

189. *Morris*, 928 F.2d at 510; Kerr, *supra* note 21, at 1631–32.

190. *Morris*, 928 F.2d at 510; Kerr, *supra* note 21, at 1631–32.

191. Goldfoot & Bamzai, *supra* note 11, at 1487.

192. *Id.* at 1490.

A PENNY FOR THEIR CREATIONS—APPRIISING USERS' VALUE OF COPYRIGHTS IN THEIR SOCIAL MEDIA CONTENT

Uri Y. Hacoheⁿ,[†] Amit Elaza^r^{††} & Talia Schwartz-Ma^o^r^{†††}

ABSTRACT

Every day, 3.5 billion social media users—among them musicians, visual artists, writers, designers, and other creators—routinely upload their creative work to social media, thereby subjecting their copyrights in those works to a laundry list of draconian demands. Although users usually retain ownership rights in their uploaded content according to most platforms' terms of service agreements, they often grant platforms unbridled license to their work that goes way beyond what is reasonably needed to operate the platform. Most licenses, for example, allow platforms to modify and commercialize their users' content and create derivative works from that content. Some licenses require users to waive claims for attribution to their works or compensation for ideas they submitted to the platforms. Finally, nearly all licenses are defined to be irrevocable (users cannot terminate them), perpetual (they last indefinitely even if the user deletes their account), and sublicensable (platforms have full discretion to extend them to third parties). Do users appreciate the breadth of the licensing agreements they grant social media platforms for original content? Would they understand them if they were to read them? Most importantly, do users care? Would they change their social media “sharing” habits or stop using a social media platform if they had more information? This final question, which focuses on the salience of user-generated content licensing terms to users—defined by the degree to which terms are sufficiently prominent in users' awareness to impact decision making—has become one of the primary benchmarks for evaluating the need for regulatory intervention in mass-market contracting. These inquiries are fundamental to the information age, when user-generated content—much of which is copyright protected—shapes culture, discourse, and communities. Nevertheless, these questions have remained surprisingly unanswered. This Article fills these gaps. It presents the results of the first comprehensive large-sample empirical study on user-generated content licensing and user attitude towards those policies. Specifically, the study investigates user

DOI: <https://doi.org/10.15779/Z38696ZZ65>

© 2021 Uri Y. Hacohe, Amit Elazari & Talia Schwartz-Maor.

† Assistant Professor, Tel Aviv University, Buchmann Faculty of Law.

†† UC Berkeley School of Law (2018).

††† UC Berkeley School of Law (2019), Hebrew University School of Law (2011). We are grateful for the Center for Technology, Society & Policy (CTSP), at the University of California at Berkeley, School of Information for supporting the research described in this paper. We are further grateful for the comments on earlier versions to Peter Menell, Deirdre Mulligan, Chris Jay Hoofnagle, Robert P. Merges, Molly Shaffer Van Houweling, Aaron Perzanowski, Eric Goldman, Casey Lynn Fiesler, Christopher Buccafusco, and the participants of the 2017 Annual Intellectual Property Scholars Conference, the 2018 Internet Law Work-in-Progress Workshop, the 2018 Bay Area Scholars Work-in-Progress Workshop. All errors remain our own.

awareness, understanding, and expectations of licensing terms and the salience of those terms to users' decisions to upload their copyrighted work. Our findings reveal significant conformity in social media platforms' licensing terms and confirm that such terms are indeed unnecessarily overbroad. Our findings also indicate that most users are unlikely to read, fully comprehend, or have realistic expectations concerning their content licensing arrangements. At the same time, our findings indicate that most users care about copyright policies and claim that they would change their social media behavior if they had more information. We then build on the study's results with law and policy insights that encompass proposals for legal policy work on consumer form contracts and intellectual property.

TABLE OF CONTENTS

| | | |
|-------------|--|------------|
| I. | INTRODUCTION | 513 |
| II. | LEGAL FRAMEWORK..... | 522 |
| A. | SOCIAL MEDIA AND THE PREVALENCE OF USER-GENERATED CONTENT | 522 |
| B. | THE COPYRIGHTABILITY OF USER-GENERATED CONTENT | 526 |
| C. | STANDARD FORM CONTRACTS AND THE COPYRIGHT BOILERPLATE | 529 |
| III. | THE STUDY..... | 531 |
| A. | OBJECTIVES AND RELATED WORK | 531 |
| B. | MAPPING THE COPYRIGHT BOILERPLATE LANDSCAPE..... | 535 |
| 1. | <i>Methods</i> | 535 |
| 2. | <i>Findings</i> | 538 |
| a) | Terms' Readability..... | 538 |
| b) | Similarity and Breadth of User-Generated Content Licensing Terms | 539 |
| C. | USERS' AWARENESS, UNDERSTANDING, AND EXPECTATIONS AND TERMS' SALIENCE SURVEY..... | 543 |
| 1. | <i>Methods</i> | 543 |
| a) | Social Media Usage | 544 |
| b) | Awareness and Understanding..... | 545 |
| c) | Expectations..... | 548 |
| d) | Salience..... | 551 |
| 2. | <i>Findings</i> | 553 |
| a) | Demographics..... | 553 |
| b) | Social Media Usage | 556 |
| c) | Awareness and Understanding..... | 558 |
| d) | Expectations..... | 565 |
| e) | Salience..... | 568 |
| 3. | <i>Methodological Limitations</i> | 576 |
| IV. | POLICY IMPLICATIONS | 577 |
| A. | MARKETS AND SELF-REGULATION..... | 580 |
| B. | SUBSTANTIVE REGULATION | 585 |

| | |
|---|------------|
| V. CONCLUSION | 594 |
| APPENDIX | 595 |
| A. COMPLETE TEXTUAL ANALYSIS OF PLATFORMS’ UGC TERMS..... | 595 |
| B. SURVEY..... | 607 |
| C. TERM AWARENESS ACROSS PLATFORMS | 613 |
| D. TERMS’ SALIENCE (RANKING)..... | 615 |

I. INTRODUCTION

Imagine you are an artist considering presenting your latest work in a local art gallery. You reach out to the gallery owner, who is excited by your query. The gallery, just like any gallery, offers you, the artist, a platform to display your artwork at no cost to you. However, here, the gallerist also sets forth several conditions for presenting your artwork in their venue. They require that you allow the gallery, as well as its affiliated business (such as the gallery’s food and beverage provider), to alter or modify your exhibited art. They also insist that you make your artwork available to advertise the gallery or any affiliate—with no additional payment to you. The gallerist further demands that the gallery and its affiliated business can do these things unilaterally and irrespective of your consent, views, or professional reputation. They will not even guarantee that the gallery will credit you as the artist. Finally, the gallerist demands to reserve their opportunity to harshen these conditions or add additional terms later, as they deem fit. Should you find these conditions objectionable in the future, you could decide not to exhibit any new art at the gallery, but any previously exhibited work would nevertheless be subject to the newly added or altered demands.

Would you choose to exhibit your artwork in such a gallery? One’s intuition about the nature of intellectual property rights, moral instincts, and basic artistic integrity might suggest that many creators are unlikely to surrender such overwhelming control over their creative output. Some may even speculate that guided by the gallerist’s offensive approach, the business is likely to fall into insolvency. Nevertheless, such outrageous licensing arrangements are standard for the millions of creative works uploaded daily.¹ Moreover, the digital “galleries” that employ such terms are anything but

1. See *infra* Section III.B; G. Ross Allen & Francine D. Ward, *Things Aren’t Always as They Appear: Who Really Owns Your User-Generated Content?*, 3 LANDSLIDE 49, 50 (2010) (“Membership in these sites is not free, albeit no fee or tax penalty is required. In return for membership, most social media sites require that the user grant the site and its third-party affiliates, now known or later established, a nonexclusive license to any UGC posted by the user.”).

insolvent businesses; instead, they are among the most thriving, wealthiest, and fastest-growing corporations in modern history.²

Today, there are about 3 billion social media users—among them musicians, visual artists, writers, designers, and other creators—who routinely upload their copyrighted output to social media platforms, thereby subjecting their rights in such works to a laundry list of draconian demands.³ While users usually retain ownership rights in their uploaded content according to most platforms' terms of service (ToS), these unbridled licenses go beyond what is reasonably needed to operate the platform.⁴

Platforms often claim a perpetual license (that would extend after users delete their account) over the right to use the work in virtually any way, including to modify, create derivative works, and utilize the work for commercial purposes.⁵ In some cases, the terms extend to a waiver of moral

2. See Macrotrends, *Facebook Market Cap 2009–2020*, <https://www.macrotrends.net/stocks/charts/FB/facebook/market-cap> (last visited Feb. 22, 2020) (providing that Facebook's market cap as of February 21, 2020 was \$611.65B); Justin Kerby, *Here's How Much Facebook, Snapchat, and Other Major Social Networks Are Worth*, SOCIALMEDIATODAY (May 16, 2017), <https://www.socialmediatoday.com/social-networks/heres-how-much-facebook-snapchat-and-other-major-social-networks-are-worth> (showing the multi-billion dollar market caps of Facebook, Snapchat, Pinterest, Twitter, LinkedIn, and YouTube); Alexis C. Madrigal, *Mark Zuckerberg's Power Is Unprecedented*, THE ATLANTIC (May 9, 2019), <https://www.theatlantic.com/technology/archive/2019/05/how-powerful-mark-zuckerberg/589129/> (“Facebook's profits land it in the top 15 companies, and its market value is in the top 10 on its perceived potential for growth.”)

3. Statista, *Number of Global Social Media Users 2010–2021*, (Aug. 14, 2019), <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>. According to some sources, there are about 3.5 billion internet users world-wide. E.g., Esteban Ortiz-Ospina, *The rise of social media*, OUR WORLD IN DATA (Sept. 18, 2019), <https://ourworldindata.org/rise-of-social-media>.

4. See *infra* Section III.B. For example, for a very long time Reddit retained a right for to use their users' content for any commercial purpose. See Reddit, *Reddit User Agreement* § 18, (effective May 27, 2016), <https://web.archive.org/web/20180405080131/https://www.reddit.com/help/useragreement/?v=ab935bec-5815-11e6-b911-0ed52af64d23> (mandating that users grant an irrevocable perpetual license to Reddit and “others” of its choice to display and reproduce their creations “in any medium and for any purpose, including commercial purpose”). This agreement was effective at least until March 2018, when Reddit changed its ToS. LinkedIn had a similar provision until October 23, 2014, noting that “[LinkedIn retains the] right to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered . . . without any further consent, notice and/or compensation.” LinkedIn, *LinkedIn Terms of Service*, (June 16, 2011), <https://web.archive.org/web/20130429153448/https://www.linkedin.com/legal/user-agreement> [hereinafter *LinkedIn Old Agreement*]. On June 7, 2017, LinkedIn made its ToS much more user friendly. See *infra* note 236–238 and accompanying text.

5. See *infra* Section III.B.2.

rights⁶ and allow the use of certain “ideas” submitted to the platform without compensation.⁷ These broad licenses permit platforms to share their users’ content in any manner, including sublicensing to third parties for commercial use.⁸ As one scholar noted, Facebook could “surreptitiously sublicense user content to porno.com,” and “this would fall squarely within the license Facebook purports to be granted by users.”⁹

Creators rarely appreciate the breadth of the license they grant a platform unless they are faced with grave implications or receive specific notice about changes in the platform’s ToS. Angel Fraley, for example, first appreciated the breadth of the license she gave Facebook in March 2011 when she saw that her profile picture appeared without her consent in a paid advertisement for a brand that Fraley “liked” on the platform.¹⁰ Similarly, Lucy Rodriguez first

6. In the United States only limited protection is granted to moral rights in creative works. The United States’ only source of moral rights, The Visual Artists Rights Act of 1990 (VARA), only grants moral rights protection to “work of visual art” under certain limitations. 17 U.S.C. § 106A(a)(3). Such rights may be waived but not transferred. *Id.* § 106A(b), (c). VARA rights do not extend to UGC that is uploaded to social media. Beatrice Kelly, *The (Social) Media is the Message: Theories of Liability for New Media Artists*, 40 COLUM. J.L. & ARTS 503, 511 (2017) (“[C]urrent moral rights legislation seems unlikely to help a digital artist. First, the [VARA] only applies to works produced in a limited edition. This requirement seems nearly impossible to overcome in the digital context, where nearly perfect copies may be endlessly replicated. Second, although there is a serious risk of technological obsolescence in Internet art, natural deterioration is not actionable under VARA.”); *see also* U.S. COPYRIGHT OFFICE, AUTHORS, ATTRIBUTION, AND INTEGRITY: EXAMINING MORAL RIGHTS IN THE UNITED STATES (2019), <https://www.copyright.gov/policy/moralrights/full-report.pdf>. In contrast, under European and international law, moral rights provide broader protection. *See generally* Berne Convention for the Protection of Literary and Artistic Works, art. 6(1), September 9, 1886, 1161 U.N.T.S. 3; ROBERTA ROSENTHAL KWALL, *THE SOUL OF CREATIVITY: FORGING A MORAL RIGHTS LAW FOR THE UNITED STATES* (2009); *see also* PETER S. MENELL, MARK A. LEMLEY, ROBERT P. MERGES, & SHYAMKRISHNA BALGANESH, 2 INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE, ch. IV, at 732 (2020).

7. *See, e.g.*, Reddit, *Reddit User Agreement*, § 4 (effective Sept. 24, 2018), <https://www.redditinc.com/policies/user-agreement-september-24-2018> (these terms were later revised as explained in Appendix A) (“Any ideas, suggestions, and feedback about Reddit or our Services that you provide to us are entirely voluntary, and you agree that Reddit may use such ideas, suggestions, and feedback without compensation or obligation to you.”). While ideas per se are not protected under the copyright laws, users might still intuitively expect some form or compensation (or at least a credit) in cases where social platforms adopt their ideas. These provisions immunize platforms from such user claims.

8. *See infra* Section III.B.2.

9. Steven Hetcher, *User-Generated Content and the Future of Copyright: Part Two—Agreements Between Users and Mega-Sites*, 24 SANTA CLARA COMPUT. & HIGH TECH. L.J. 829, 848–49 (2008).

10. *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 792 (N.D. Cal. 2011) (explaining that once Fraley “liked” Rosetta Stone’s Facebook profile page, the platform posted her Facebook user name and profile picture on her Friends’ Facebook pages in a “Sponsored Story” advertisement consisting of the Rosetta Stone logo and the sentence, ‘Angel Frolicker likes

appreciated the breadth of Instagram's license in February 2014 when the platform sent her a specific notice detailing its intent to introduce new and harsher demands to its ToS. For example, the new terms authorized Instagram to sublicense users' content, removed limitations from users' licenses, and forced users to waive liability claims.¹¹

Irrespective of the platforms' broad prerogative to exploit users' creative works, the integrity of such works may also be compromised by the acts of third-party users whose access to that content is hardly restricted.¹² For example, on January 2010, a Cypriot refugee and photographer named David Kittos discovered Donald Trump Jr. used in a tweet critical of refugees a photograph that Kittos took and made available on Flickr.¹³ Similarly, in May

Rosetta Stone.'"). This class action later settled. For further discussion, see Jesse Koehler, *Fraleigh v. Facebook: The Right of Publicity in Online Social Networks*, 28 BERKELEY TECH. L.J. 963 (2013).

11. See *Rodriguez v. Instagram L.L.C.*, No. 3:12-cv-06482-WHA, at 6 (N.D. Cal. Mar. 6, 2013).

12. As one commenter mentioned, users are "led to believe that delete equals delete, yet the very nature of social networking is the 'sharing' concept. So if a user shares her content with 500 of her 'friends,' and then decides to delete the content, those 500 friends still have access to the content; therefore, it is not deleted." Allen & Ward, *supra* note 1, at 50; see Joe Brown, *Instagram's New Terms of Use, Translated into Plain English*, GIZMODO (Jan. 18, 2013), <https://gizmodo.com/instagrans-new-terms-of-use-translated-into-plain-engl-5977053> ("[E]ven if you delete, deactivate, or terminate your account, your stuff might still live on Instagram like a zombie."). Most platforms are compelled by the copyright statute to maintain a notice and takedown mechanism to help users to combat potential copyright violations on their sites. 17 U.S.C. § 512 (c)(1)(A)(1998). Of course, if users download creative works and violate copyright elsewhere, the responsibility to enforce these rights are left to the user. See Jessica Contrera, *A reminder that your Instagram photos aren't really yours: Someone else can sell them for \$90,000*, WASH. POST (May 25, 2015), <https://www.washingtonpost.com/news/arts-and-entertainment/wp/2015/05/25/a-reminder-that-your-instagram-photos-arent-really-yours-someone-else-can-sell-them-for-90000/> ("On the platform, if someone feels that their copyright has been violated, they can report it to us and we will take appropriate action. Off the platform, content owners can enforce their legal rights.").

13. According to the media reporting, Trump Jr. tweeted the image of multicolored candy inside a white bowl 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." Chiara Palazzo, *Donald Trump Jr Compares Syrian Refugees to a Bowl of Skittles*, THE TELEGRAPH (Sept. 20, 2016), <http://www.telegraph.co.uk/news/2016/09/20/donald-trump-jr-compares-syrian-refugees-to-a-bowl-of-skittles/>. Kittos filed a takedown notice under the DMCA, the tweet was removed, and a copyright infringement suit was initiated in Illinois Northern District Court but then dropped. See *Kittos v. Donald J. Trump For President, Inc.*, No. 1:2016cv09818 (N.D. Ill. Oct. 18, 2016).

Flickr users generally retain rights to their uploaded copyrighted works by default under the Flickr license. Flickr also allows users to waive their rights to their works but only if they elect to do so affirmatively. See *Change Your Photo's License in Flickr*, FLICKR HELP,

2015, several Instagram users were astonished to discover printed screenshots of their Instagram photographs hanging at the Frieze Art Fair in New York City as part of an exhibition by the famous appropriation artist Richard Prince,¹⁴ priced at \$90,000 apiece.¹⁵

Do creators know what rights they have in their uploaded content? Do they know how much of these rights they are giving away? Do they care? These questions are fundamental to the information age, where culture, discourse, and communities are shaped by user-generated content (UGC),¹⁶ and much of this content is copyright protected.¹⁷ Nevertheless, such inquiries remain surprisingly unanswered thus far. Indeed, in the wake of the Cambridge Analytica and foreign-influence scandals surrounding the 2016 presidential election, a surge of legal scholarship began scrutinizing social media giants with an eye toward users' privacy,¹⁸ autonomy,¹⁹ and free speech.²⁰ Policymakers,

https://help.flickr.com/en_us/change-your-photo's-license-in-flickr-B1SxTmjKX (last visited Feb. 25, 2020).

14. Lisa Respers France, *Photographer sells others' Instagram photos as art*, CNN (May 29, 2015), <https://www.cnn.com/2015/05/27/living/richard-prince-instagram-feat/index.html>; Contrera, *supra* note 12.

15. France, *supra* note 14.

16. Indeed, in defining UGC, commenters have consistently recognized the elements of creativity and self-expression. *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) (“UGC is creative content produced and published, usually by individuals who possess limited technical expertise, out of a desire to share, connect with others, or simply to express oneself.”); Mihajlo Babovic, *The Emperor's New Digital Clothes: The Illusion of Copyright Rights in Social Media*, 6 CYBARIS AN INTELL. PROP. L. REV. 138, 143 (2015) (“User-generated content, then, means that the individual or organization has created, produced, or developed the content—the phrase in itself would seem to contain an implicit level of creativity.”). According to the Organization for Economic Cooperation and Development, UGC should reflect (among other requirements) “a certain amount of creative effort.” Sacha Wunsch-Vincent & Graham Vickery, PARTICIPATIVE WEB: USER-CREATED CONTENT 8 (2007), <https://www.oecd.org/digital/ieconomy/38393115.pdf>. For a general discussion on how UGC transformed culture and society, see Jack M. Balkin, *Cultural Democracy and the First Amendment*, 110 Nw. U. L. Rev. 1053 (2016) (emphasizing how digitalization empowered cultural theory beyond traditional democracy-based theories); YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* (2006) (describing how user-generated creativity and collaboration transform economics and culture).

17. *See infra* Section II.B.

18. *See infra* notes 93–94 and accompanying text.

19. *See* SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* (2019) (setting forth the theory that the rise of the surveillance economy comes at the expense of human autonomy).

20. *See, e.g.*, CASS R. SUNSTEIN, *#REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA, IX* (2017) (arguing that platforms' tendency to personalize user experience creates “filter bubbles” which goes against the values embedded in the Fourth Amendment, namely the significance of a diverse and vibrant “public sphere” which is free from speech

legislators, and social activists offered to boycott social media platforms,²¹ regulate them,²² or harness the competition authorities to break them down.²³ In the midst of this passionate policy debate, concerns about users' copyrights in their UGC were all but overlooked.²⁴ This Article is meant to fill this gap by presenting the results of the first comprehensive study to investigate social media platforms' UGC licensing policies.

The study has two parts. It begins by mapping and comparatively analyzing the UGC licensing provisions of eleven of the most popular social media platforms for terms' similarity, readability, and breadth. It then presents the results of a survey (N=1,033) designed to investigate social media users'

restrictions, and stating “the system of free expression must do far more than avoid censorship; it must ensure that people are exposed to competing perspectives. The idea of free speech has an affirmative side. It imposes constraints on what government may do, but it requires a certain kind of culture as well—one of curiosity, openness, and humility.”); Daphne Keller, *Facebook Restricts Speech by Popular Demand*, THE ATLANTIC (Sept. 22, 2019), <https://www.theatlantic.com/ideas/archive/2019/09/facebook-restricts-free-speech-popular-demand/598462/> (exploring Facebook speech regulation practices and claiming that “[t]he prevailing framework for free expression is getting a do-over.”).

21. See, e.g., Jon Swartz, *Wikipedia co-founder plans two-day social-media boycott*, MARKETWATCH (July 3, 2019), <https://www.marketwatch.com/story/wikipedia-co-founder-plans-two-day-social-media-boycott-2019-07-03>.

22. See, e.g., Cecilia Kang & Kevin Roose, *Zuckerberg Faces Hostile Congress as Calls for Regulation Mount*, N.Y. TIMES, (Apr. 11, 2018), <https://www.nytimes.com/2018/04/11/business/zuckerberg-facebook-congress.html> (examining the growing calls to regulate Facebook); see also Nina Jankowicz, *Opinion: It's time to start regulating Facebook*, WASH. POST, <https://www.washingtonpost.com/news/democracy-post/wp/2018/11/15/its-time-to-start-regulating-facebook/> (last visited Nov 25, 2020); Mike Allen & Ina Fried, *Apple CEO Tim Cook Calls New Regulations “Inevitable”*, AXIOS (Nov. 18, 2018), <https://www.axios.com/axios-on-hbo-tim-cook-interview-apple-regulation-6a35ff64-75a3-4e91-986c-f281c0615ac2.html>; Natasha Tusikov & Blyne Haggart, *It's Time For A New Way To Regulate Social Media Platforms*, THE CONVERSATION (Jan. 16, 2019) <http://theconversation.com/its-time-for-a-new-way-to-regulate-social-media-platforms-109413>.

23. See, e.g., Siva Vaidhyanathan, *Opinion | Don't Delete Facebook. Do Something About It*, N.Y. TIMES (June 8, 2018), <https://www.nytimes.com/2018/03/24/opinion/sunday/delete-facebook-does-not-fix-problem.html> (“The Department of Justice should consider severing WhatsApp, Instagram and Messenger from Facebook, much as it broke up AT&T in 1982. That breakup unleashed creativity, improved phone service and lowered prices. It also limited the political power of AT&T.”); Nilay Patel, *It's Time to Break Up Facebook*, THE VERGE (Sept. 4, 2018), <https://www.theverge.com/2018/9/4/17816572/tim-wu-facebook-regulation-interview-curse-of-bigness-antitrust>; Damian Tambini, *What Should Be Done With Facebook—Break It Up, Or Regulate It?*, THE GUARDIAN (Apr. 27, 2018), <http://www.theguardian.com/commentisfree/2018/apr/27/facebook-regulate-tech-platforms> (“[Regulators] can use the tax system: the problem is that we do not have a sense of whether Facebook is more like the alcohol and gambling industries—which are considered a social bad and taxed accordingly—or a social good and subject to tax breaks.”).

24. See *infra* Section III.A.

awareness, understanding (whether they comprehend), and expectations (what they want) of the copyright-licensing terms that govern their uploaded UGC. Finally, and most significantly, this study questions the *salience* of UGC licensing terms to users—the degree to which users’ awareness, understanding, and expectations are manifested into actions that impact users’ contractual decisions and content-uploading habits.²⁵

Our findings paint a troubling picture. The textual analysis portion of our study concludes that the UGC licensing policies of many leading platforms appear in a boilerplate form and are grossly overbroad in a way that might undermine the goals of copyright law.²⁶ Our survey portion’s findings are similarly concerning. First, our data suggest that a sizable percentage of social media creators do not understand which rights they have in their UGC to begin with. For example, 31% of the survey participants did not understand the meaning of “derivative work” (a statutory right licensed under the ToS of most platforms in our dataset).²⁷ These findings suggest that social media users routinely trade with property rights that they do not even know exist.²⁸

25. The principle of “salience” is the predominant emerging paradigm to evaluate the legitimacy of standard-form contractual terms. *See* RESTATEMENT OF THE L. CONSUMER CONTS., § 5 notes at 94–95 (AM. L. INST., Tentative Draft 2019), https://www.ali.org/media/filer_public/05/30/053007a1-2b37-4142-b9c3-7a881e847d50/consumer_contracts_-_td_-_online.pdf; Amit Elazari Bar On, *Unconscionability 2.0 and the IP Boilerplate: A Revised Doctrine of Unconscionability for the Information Age*, 34 BERKELEY TECH. L.J. 567, 624–29 (2019). The U.C.C. adopts the salience test articulated by the above Restatement. *See* U.C.C. § 2-316(2) & cmt. 1 (AM. L. INST. & UNIF. LAW COMM’N 2020). (excluding an implied warranty requires “conspicuous” writing free of “unexpected and unbargained language of disclaimer”). Still, it should be noted that the Restatement adopted the notion of salience in the Reporters’ notes and not the “black letter” or commentary parts. RESTATEMENT OF THE L. CONSUMER CONTS., § 5 notes at 97–98. The notion of salience was first broadly introduced in Russell Korobkin’s *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203 (2003). According to Korobkin, consumers’ ability to price contractual terms in their entirety is limited because they are “boundedly rational decisionmakers.” *Id.* at 1203. Consumers are “bounded” because they simply do not have the economic incentive to invest the time required to understand and evaluate all terms. *Id.* Because the market does not police the quality of potentially “socially inefficient” terms, these “nonsalient” terms, which are not evaluated by a significant number of buyers, must be regulated. *Id.* 1203–06; *see also* Part IV. Indeed, according to the Restatement, “standard terms are *prima facie* nonsalient” and thus “courts adjudicating an unconscionability claim can focus their attention on the substantive inquiry.” RESTATEMENT OF THE L. CONSUMER CONTS., § 5 notes at 97. As we explain, such inquiry can focus on, *inter alia*, how a term might undermine the purpose of intellectual property laws or rights impacted by the proposed contractual term. *See* Section IV(B); Elazari Bar On, *supra* note, at 657.

26. *See infra* notes 244–247 and accompanying text.

27. *See infra* Section III.C.2.c).

28. *See infra* notes 244–247 and accompanying text. One might even argue that because social media platforms thrive on UGC they have a moral duty, if nothing else, to make sure

Second, and in line with recent empirical investigation of digital contracts generally, our data indicate that a sizable percentage of social media users are unaware of and falsely optimistic about the scope of the licenses they grant social media platforms.²⁹ For example, only 20% of all respondents indicated that they thought social media platforms can grant third parties a license to use their work; yet all the ToS in our dataset at the time of the survey enabled platforms to do just that.³⁰ Similarly, merely 25% of respondents thought that social media platforms are allowed to modify their work, something most platforms can do according to their ToS.³¹

Third, our data also indicate that users' expectations—what should be, in their opinion, the ideal scope of UGC license—diverge substantially from reality. For example, 49.7% of the survey recipients indicated that their work should be available *only* for as long as they “agree,” while only 3.4% indicated that they wish their work to be available indefinitely.³² The terms of nearly all the platforms in our dataset, however, specifically provide perpetual UGC licenses that would technically allow platforms to display and distribute users' content indefinitely.³³

Fourth, and most importantly, in contrast to privacy critics' conventional wisdom that users simply do not care about their rights or would willingly trade these rights for free services,³⁴ our data clearly suggest that most users care

that users are fully aware of their rights and are willfully participating in the service. *Cf.* Elizabeth Townsend Gard & Bri Whetstone, *Copyright and Social Media: A Preliminary Case Study of Pinterest*, 31 MISS. C. L. REV. 249, 275 (2012) (“Since users are the bread and butter of social media sites . . . these sites should at least take the responsibility of writing Terms of Service in easy to understand concepts. Copyright never has to be scary if sites are transparent about what rights they claim and users' responsibilities in terms of content.”).

29. *Cf.* Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 551 (2014) (“[T]erm optimism? . . . exists when consumers expect a contract to contain more favorable terms than it actually provides.”).

30. *See infra* Section III.C.2.c).

31. *Id.*

32. *See infra* Section III.C.2.d).

33. *See infra* Section III.C.2.d).

34. *See* James C. Cooper & Joshua D. Wright, *The Missing Role of Economics in FTC Privacy Policy*, in CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 22 (Jules Polonetsky, Evan Selinger & Omer Tene eds., 2017) (“[M]ost consumers are comfortable with the typical bargain of sharing information with faceless servers in return for free content and services, such as email and social networking platforms.”); *but see* Daniel J. Solove, *The Myth of the Privacy Paradox* (Feb. 1, 2020), <https://ssrn.com/abstract=3536265> (discussing, and refuting, the “privacy paradox” phenomenon—while some claim they value privacy highly, their actual behavior suggests otherwise: they relinquish their data or do not proactively safeguard their privacy). Solove claims that “the privacy paradox is a myth created by faulty logic” since privacy paradox empirical studies involve very specific contexts whereas users' privacy attitudes are actually

deeply about the legal rights in their creative content and would potentially rethink their sharing behavior if they possessed more information. For example, the vast majority of respondents (78.7%) indicated that they are unlikely (34.56%) or extremely unlikely (44.14%) to use a platform whose terms authorizes third parties to distribute or modify user work—something that all the platforms in our dataset currently require.³⁵ Faced with similar findings in the privacy arena, commenters coined the term “privacy paradox” to describe users’ tendency to behave in direct conflict to their expressed preferences.³⁶ Our data reveal a comparable “UGC licensing paradox.”

Finally, our findings provide surprising insight into which rights users consider the most valuable to them. For example, most respondents have indicated that having their work associated with their name—commonly known as the right of attribution, which is not respected for uploaded content under U.S. law³⁷—is even more valuable to them than having their work protected from modification or commercialization by the platform.³⁸ These findings can assist policymakers (and social media platforms) in reconsidering user rights in the digital age.

This Article includes three main parts. Part II presents the applicable legal framework: Section A explores the rise of social media and its dependence on

more general in nature. *Id.* at 2. Thus, Solove observes that data in specific contexts should not be used to reach broader conclusions. *Id.*; see also *infra* notes 93–95 and accompanying text (discussion concerning the “Privacy Paradox”).

35. See *infra* Section III.C.2.e).

36. See, e.g., Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509, 510 (2015) (“This discrepancy between attitudes and behaviors has become known as the ‘privacy paradox.’”); Meredydd Williams, Jason R. C. Nurse & Sadie Creese, *The Perfect Storm: The Privacy Paradox and the Internet-of-Things*, 2016 11th INT’L CONF. ON AVAILABILITY, RELIABILITY & SEC. 644, 644 (2016) (“While many individuals claim to care about privacy, they are often perceived to express behaviour to the contrary. This phenomenon is known as the Privacy Paradox.”); Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, MIT SLOAN RESEARCH PAPER NO. W23488 (2017), https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141392.pdf (finding that users who mentioned they feel strongly about not sharing their contacts’ information were happily willing to do just that moments later when offered a free pizza slice in exchange for their friends’ email addresses); Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100, 110–13 (2007) (finding that users shared nearly twice as more personal information than what they stated they were willing to share); Kenneth A. Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On & Irwin Reyes, *Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps*, 35 BERKLEY TECH. L.J. 327, 331 (“The misdirection of privacy policies and the framing effects of the ‘myth’ of free, moreover, exacerbate the “privacy paradox[.]”).

37. See *supra* note 6.

38. See *infra* Section III.C.2.e).

UGC; Section B explains that a substantial portion of the uploaded UGC is copyright protected; and Section C discusses the copyright licensing practice. Part III presents our study: Section A sets out the study's objectives and summarizes related work; Section B maps and analyzes the ToC copyright term landscape; and Section C describes our ToS awareness, understanding, expectations, and overall salience survey. Finally, Part IV discusses the policy implication of our findings: Section A discusses the role of market pressure and self-regulation, and Section B investigates avenues for substantive regulation of UGC licensing terms.

II. LEGAL FRAMEWORK

A. SOCIAL MEDIA AND THE PREVALENCE OF USER-GENERATED CONTENT

When it first emerged in the mid-1900s, the internet (then known as the ARPANET) was a research network run by the Department of Defense and connecting only a few universities.³⁹ During these early days, most users were visiting the Web and not contributing to it; the conceptualization of the internet as a place of social connectivity, cultural dialogue, and collaborative “platform-based” creativity seemed fictional.⁴⁰ But by the beginning of the 21st century, standards, protocols, and institutions managing the internet improved, and more websites offered usability and interoperability for end users. These changes transformed the Web from “read-only” (Web 1.0) to “read and write” (Web 2.0).⁴¹ In this environment, users’ contribution and

39. See, e.g., MATTHEW CRICK, POWER, SURVEILLANCE, AND CULTURE IN YOUTUBE'S DIGITAL SPHERE 4 (IGI Global, 2016) (discussing the Web's history).

40. See B. K. Hiremath & Anand Y. Kenchakkanavar, *An Alteration of the Web 1.0, Web 2.0 and Web 3.0: A Comparative Study*, 2(4) IMPERIAL JOURNAL OF INTERDISCIPLINARY RESEARCH, 705 (2016) file:///C:/Users/uriha/Desktop/138.pdf (last visited Nov 25, 2020) (reviewing the early evolution of the web and arguing that the emergence of Web 2.0 is “absolutely the subsequently big thing in the World Wide Web.”); Mike Wolcott, *What Is Web 2.0?*, CBS NEWS, http://www.cbsnews.com/8301-505125_162-51066094/what-is-web-20/ (last visited Nov 25, 2020) (arguing that the Web 2.0 revolution “represents an important shift in the way digital information is created, shared, stored, distributed, and manipulated,” and that this revolution “will have a significant impact in the way businesses use both the Internet and enterprise-level IT applications.”).

41. See Tim O'Reilly, *What is Web 2.0: Design patterns and business models for the next generation of software*. O'REILLY RADAR. Retrieved from: <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>, 2005; see also Pamela Samuelson, *Freedom to Tinker*, 17 THEORETICAL INQUIRIES LAW 563, 564 (2016) (“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

collaboration took center stage.⁴² To celebrate this transformation, *Advertising Age* magazine named “the consumer” as its 2006 “agency of the year,”⁴³ *Time* magazine selected the consumer as “person of the year,”⁴⁴ and various commenters applauded the empowerment of end-users and amateur creators.⁴⁵

Social media platforms were leading players in this revolution. They allowed users to construct public or semipublic profiles that were visible to other users and allowed peers to communicate, create, and share content with one another.⁴⁶ Driven by market competition and their unique “attention-based” business models, platforms strived to reward users for deepening their

others.”). 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, 312–13 (2014) (“Digital 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 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 . . .”).

42. *Supra* note 42.

43. Matthew Creamer, *John Doe Edges out Jeff Goodby*, ADVERTISING AGE (Jan. 8, 2007), at S-4.

44. Lev Grossman, *Person of the Year: You*, TIME (Dec. 25, 2006), <http://content.time.com/time/magazine/article/0,9171,1570810,00.html> (explaining that “you” are the founders of Web 2.0 and the new era of “digital democracy”); *see also* Jeff Howe, *Your Web, Your Way*, TIME (Dec. 25, 2006), at 60 (briefly overviewing peer-generated content, using the term “crowdsourcing”).

45. *See, e.g.*, Ellen P. Goodman, *Peer Promotions and False Advertising Law*, 58 S.C. L. REV. 683 (2007) (explaining how the enhanced role of peer commentary has revolutionized advertising law); Zahr Said, *Embedded Advertising and the Venture Consumer*, 89(1) N.C. L. REV. 99 (2010) (arguing that consumers in the digital age are empowered and exploring the impact of this empowerment on advertising regulation policy); BENKLER, *supra* note 16 at 129 (describing the impact of peer networks on political and individual freedoms); CASS R. SUNSTEIN, *INFOTOPIA: HOW MANY MINDS PRODUCE KNOWLEDGE* 148–49 (2006) (emphasizing the ability of any user to create and edit content online); Dan Hunter & F. Gregory Lastowka, *Amateur-to-Amateur*, 46 WM. & MARY L. REV. 951, 979–89 (2004) (describing instances of “unauthorized amateur authorship” and “new forms of collaborative creativity”); Creamer, *supra* note 43, at S-4.

46. Andreas M. Kaplan & Michael Haenlein, *Users of the World, Unite! The Challenges and Opportunities of Social Media*, 53 BUS. HORIZONS 59, 61 (2010) (defining social media as “a group of Internet-based applications . . . that allow the creation and exchange of User Generated Content”); Crick, *supra* note 39, at 28; Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 (1) J. COMPUT.-MEDIATED COMM'N, 210, 211 (2007), (defining social network sites as web-based services that allow individuals to (1) construct profiles; (2) connect with other users; and (3) view and traverse their and others’ list of connections within the system).

engagement with the platforms' services.⁴⁷ The ability to personalize a webpage with unique backgrounds and images and to "copy and paste" code, for example, were two early technologies developed by MySpace, which led to the site's rise in popularity and the end of social media platform Friendster.⁴⁸ Over time, UGC substituted customized design as a means to attract users and personalize their social media experience. Soon, platforms that emphasized creating and sharing UGC, such as Facebook, Instagram, and Twitter, became industry leaders.⁴⁹

To improve services and grow their user base, social media platforms also encouraged users to generate and share content indirectly simply by revolutionizing the world of digital advertising. By fostering cheap and real-time connectivity among consumers, platforms advanced the wide-ranging methodological shift from a "one-way street" advertising philosophy, which befitted print and broadcast media, to a newer "two-way street" philosophy emphasizing consumer collaboration, contribution, and co-creation.⁵⁰ The new advertising approach specifically required users to create and share creative

47. Because platforms provide "free" services while making profits from targeted advertising, platforms strive to maximize connectivity (which leads to more advertising exposure) and user engagement (which leads to better targeting capabilities). For a detailed exploration of this unique business model. See Zuboff, *supra* note 19.

48. See Crick, *supra* note 39, at 28.

49. See Cameron Chapman, *The History and Evolution of Social Media*, WEBDESIGNER DEPOT (Oct. 7, 2009), <https://www.webdesignerdepot.com/2009/10/the-history-and-evolution-of-social-media/> (last visited Jan. 14, 2020) ("In 2008 Facebook became the most popular social networking site, surpassing MySpace, and continues to grow. Facebook doesn't allow the same kind of customization that MySpace does. Facebook does, however, allow users to post photos, videos and otherwise customize their profile content, if not the design."); Jessica Gutierrez Alm, "Sharing" Copyrights: *The Copyright Implications of User Content in Social Media*, 35 HAMLINE J. PUB. L. & POL'Y 104, 106 (2014) ("Early social media leaders like Facebook, YouTube, and Twitter originally focused on user-generated content by offering platforms where users could post images, videos, and writings they create."). Instagram, for example, according to its CEO and co-founder, Kevin Systrom, was focused since the beginning on "inspiring creativity" and "becom[ing] the home for visual storytelling for everyone." See Instagram, *About Us*, <https://www.instagram.com/about/us/> (last visited Feb. 25, 2020).

50. "Co-creation" is defined as a collaboration between the consumer and the marketer to shape brand meaning. See, e.g., CLAUDIU V. DIMOFTE, CURTIS P. HAUGTVEDT, & RICHARD F. YALCH, CONSUMER PSYCHOLOGY IN A SOCIAL MEDIA WORLD 135 (2015) (discussing co-creation and noting that 85% of marketers consider brand co-creation investments to take advantage of social media opportunities); V. Kumar & Shaphali Gupta, *Conceptualizing the Evolution and Future of Advertising*, 45(3) J. ADVERTISING, 302, 303 (2016) ("Marketers moved from a product focus to a sales focus, to eventually a relationship focus. The focus shifted to developing and disseminating communication that inspired consumers to not merely buy but form a lasting relationship with the brand.").

content on social media.⁵¹ Users were incentivized by contests, prizes, and peer recognition.⁵² We are all familiar with these campaigns. In 2015, for example, the retail company Nasty Gal asked users to take selfies with strangers and post them on Instagram for the chance to win a Nasty Gal gift card.⁵³ Other types of promotional endeavors inspire users to create and share content more subtly by inviting them to react and interact with “viral” advertisements.⁵⁴ Successful campaigns such as Dairy Milk’s drumming gorilla⁵⁵ or Old Spice’s “The Man Your Man Could Smell Like,”⁵⁶ for example, have triggered a

51. See, e.g., Deepa Seetharaman, *Facebook Prods Users to Share a Bit More*, WALL STREET JOURNAL, November 13, 2015, <https://www.wsj.com/articles/facebook-prods-users-to-share-a-bit-more-1446520723> (last visited Nov 4, 2020) (explaining how Facebook nudges users to post content).

52. See, e.g., Rebecca Tushnet, *Attention Must Be Paid: Commercial Speech, User-Generated Ads, and the Challenge of Regulation*, 58 BUFFALO L. REV. 722, 738 (“Volunteer salespeople have also emerged by design, with traditional marketers soliciting user-generated ads for their products and showcasing the most persuasive ones in various ways.”); Goodman, *supra* note 45, at 684–85 (footnotes omitted) (“The power of the peer-to-peer model of production is changing the way advertisers think about communications and how much control they are willing to yield over brand management. As consumers express their devotions to brands in blogs, wikis, video-sharing sites like YouTube, and social networking sites like MySpace and Facebook, brand owners monitor, exploit, and sometimes imitate the genre.”).

53. See Jim Belosic, *How to Run an Instagram Contest: Four Easy Steps*, SOCIAL MEDIA EXAMINER (Feb. 17, 2015), <https://www.socialmediaexaminer.com/run-an-instagram-contest-four-easy-steps/> (last visited Dec. 27, 2020). Other co-creation campaigns are more complex. LEGO®, for example, invited users to create novel LEGO constructions and to promote their designs on social media. LEGO then promised to convert one of the most liked designs into a real-world salable playset and to give the winning designer a percentage of the product’s sales. See Albizu Garcia, *How Co-Creation is Fueling The Future of Marketing*, SOCIAL MEDIA TODAY, <https://www.socialmediatoday.com/marketing/how-co-creation-fueling-future-marketing> (last visited Nov. 5, 2018). See generally, Hacohen & Menell, *supra* note 47.

54. Electronic referral marketing (ERM) or “viral marketing” is another form of marketing technique that emphasizes user engagement. See Arnaud De Bruyn & Gary L. Lilien, *A Multi-Stage Model of Word-of-Mouth Influence Through Viral Marketing*, 25 INT’L J. RES. MARKETING, 151, 151–52 (2008) (defining electronic referral marketing (ERM) as the use of electronic “consumer-to-consumer . . . communications—as opposed to company-to-consumer communications—to disseminate information about a product or service, thereby leading to more rapid and cost effective adoption by the market”); Robert Allen King, Pradeep Racherla & Victoria D. Bush, *What We Know and Don’t Know About Online Word-of-Mouth: A Systematic Review and Synthesis of the Literature*, 28 JOURNAL OF INTERACTIVE MARKETING 167, 170 (2014) (defining enhanced volume as one of the main dynamics that drive electronic word-of-mouth communications); Maria Petrescu, Kathleen O’Leary, Deborah Goldring & Selima Ben Mrad, *Incentivized reviews: Promising the moon for a few stars*, 41 J. RETAILING & CONSUMER SERVICES 288, 288–95 (2018) (“Word-of-mouth marketing is a brand-initiated strategy of intentionally persuading consumer-to-consumer conversations.”).

55. Roberto Becerra, *Phil Collins Gorilla Drummer Cadbury Ad Dairy Milk*, YOUTUBE (April 29, 2013), <https://www.youtube.com/watch?v=kAOZ14Tjg7A> (last visited Feb. 25, 2020).

56. Old Spice, *The Man Your Man Could Smell Like*, YOUTUBE (Feb. 4, 2010) <https://www.youtube.com/watch?v=owGykVbfgUE> (last visited Nov. 9, 2018).

massive volume of UGC in the form of parodies, spoofs, and textual commentary.⁵⁷

Unsurprisingly, the amount of shared UGC on social media is massive. According to the consumer marketing platform Annex Cloud, for example, in 2016, users uploaded between 2 to 4 billion images to social media per day, and the number of user uploaders had increased by 176 million compared to the previous year.⁵⁸ This uploaded content is subject both to federal copyright law and contract law governing the user-platform agreements. The next two Sections discuss these legal regiments, respectively.

B. THE COPYRIGHTABILITY OF USER-GENERATED CONTENT

To be protected, creative work must satisfy the copyright's statutory requirements of originality and fixation.⁵⁹ It is reasonable to assume that a substantial portion of the UGC that is shared on social media will satisfy these two conditions.⁶⁰ The fixation prong will be satisfied for any UGC that is

57. See Karen Attwood, *Drumming gorilla aids revenues at Cadbury*, THE INDEPENDENT (Dec. 12, 2007), <http://www.independent.co.uk/news/business/news/drumming-gorilla-aids-revenues-at-cadbury-764705.html> (last visited Jan. 13, 2020) (“There have been more than 600 postings of the ad and spoofs on YouTube and the videos have been viewed more than 10 million times online.”); Megan O’Neill, *Top 10 Old Spice Parodies On YouTube*, ADWEEK (July 19, 2010) <https://www.adweek.com/digital/top-10-old-spice-parodies-on-youtube/> (last visited Jan. 13, 2020) (“Every [sic] since Old Spice’s ‘The Man Your Man Could Smell Like’ commercials hit YouTube, they’ve inspired a whole slew of spoofs, parodies and remixes.”). These creations were then shared on platforms such as YouTube to generated even more user reaction and commentary. See Brenna Ehrlich, *Lessons Learned From The Old Spice Campaign & Its Imitators*, MASHABLE (Mar. 16, 2011) <https://mashable.com/2011/03/16/old-spice-imitators/> (last visited Oct. 16, 2019) (“One of the reasons why the Old Spice campaign went so viral was that it targeted folks who were influential in the online sphere . . . Those people then acted as brand advocates [j]spreading the gospel of Old Spice to their followers.”); see also Brenna Ehrlich, *The Old Spice Guy Now Making Custom Videos for Fans via Social Media*, MASHABLE (July 13, 2010), <https://mashable.com/2010/07/13/old-spice-gu/> (last visited Oct. 16, 2019).

58. Sean Ogino, *The Ultimate List of User Generated Content Statistics*, ANNEX CLOUD (Sep. 1, 2016) <https://www.annexcloud.com/blog/the-ultimate-list-of-user-generated-content-statistics/> (last visited Jan. 14, 2020); see also Jim Edwards, *Planet Selfie: We’re Now Posting a Staggering 1.8 Billion Photos Every Day*, BUS. INSIDER (May 28, 2014), <http://www.businessinsider.com/were-now-posting-a-staggering-18-billion-photos-to-social-media-every-day2014-5> (Facebook, Instagram, Flickr, Snapchat, and WhatsApp users alone “upload[ed] 1.8 billion images . . . every day”).

59. 17 U.S.C. § 102(a) (2013) (limiting copyright-eligible works to “original works of authorship fixed in any tangible medium of expression”).

60. See Gutierrez Alm, *supra* note 49, at 107 (“Much of this user-generated content may be copyrightable.”); Babovic, *supra* note 16, at 144 (“[A]s a baseline, user-generated content can be copyrightable”). Many copyright infringement cases involve UGC. See, e.g., Perfect 10,

uploaded because, as soon as such content becomes available to other users, it is “perceived, reproduced, or otherwise communicated,” even if for a temporary period of time.⁶¹ The originality prong, on the other hand, would not always be met.⁶² Nevertheless, the standard for copyright originality is so famously low⁶³ that even works of negligible creative expression, such as many status updates on Facebook or 140-character tweets, might satisfy it.⁶⁴

Indeed, most UGC would have at least the modicum of minimal creativity judicially required to satisfy the originality prong.⁶⁵ Selfies, defined by *Time Magazine* as a modern self-portrait, taken at odd angles via smartphone and often shared through social media, are perhaps the most intuitive example.⁶⁶ In recent years, selfies became a cultural phenomenon of international

Inc. v. Giganews, Inc., 993 F. Supp. 2d 1192 (C.D. Cal. 2014) (questioning whether a bulletin board website that hosted infringing photographs could receive immunity under the Digital Millennium Copyright Act’s (DMCA) § 512 safe harbor provision); Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724 (S.D.N.Y. 2012) (concerning the application of the § 512 safe harbor provision to the website Photobucket); Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150 (N.D. Cal. 2008) (concerning a YouTube user video defended as fair use against a claim of copyright infringement).

61. MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518–19 (9th Cir. 1993) (quoting 17 U.S.C. § 101 (2012)); London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153, 171 (D. Mass. 2008) (holding that a sound recording downloaded through a peer-to-peer file sharing service was deemed fixed); Babovic, *supra* note 16, at 144 (arguing that UGC satisfies that fixation requirement).

62. See, e.g., Babovic, *supra* note 16, at 145–48 (discussing problems of merger and length).

63. Feist Pubs., Inc. v. Rural Tel. Svc. Co., Inc. 499 U.S. 340, 345 (1991) (citing 1 M. NIMMER, NIMMER ON COPYRIGHT § 108[c][1] (1988)) (“[Requiring only] some creative spark, ‘no matter how crude, humble, or obvious’ it might be.”).

64. See Babovic, *supra* note 16, at 148 (“[A] user who recounts a story via a Facebook status update could claim copyright ownership to that writing . . . even a joke being told via Twitter can certainly possess the originality required to receive copyright protection in the work.”); Stephanie Teebagy North, *Twitterright: Finding Protection in 140 Characters or Less*, 11 J. HIGH TECH. L. 333, 335 (2011) (arguing that while the majority of tweets are likely non-copyrightable, some are likely to be protected); Consuelo Reinberg, *Are Tweets Copyright-Protected?*, WIPOMAGAZINE (July 2009), http://www.wipo.int/wipo_magazine/en/2009/04/article_0005.html (same); see also Gutierrez Alm, *supra* note 49, at 110 (“There are great works, of which copyright protection is unquestioned, that would fit comfortably within Twitter’s 140-character limit”).

65. See Feist 499 U.S. at 341.

66. See Katy Steinmetz, *The Top Ten Buzzwords of 2012*, TIME (Dec. 4, 2012), <http://newsfeed.time.com/2012/12/04/top-10-newslists/slide/selfie/>, archived at <http://perma.cc/67BG-55L8>. Although, to date, the term “selfie” has largely escaped judicial attention, the first legal opinion to define the term used the definition provided by the Time article; see also United States v. Doe, No. 1:12-cr-00128-MR-DLH, 2013 WL 4212400, at 8, n.6 (W.D.N.C. Aug. 14, 2013) (quoting Time Magazine’s description of “selfies.”)

magnitude.⁶⁷ A 2013 survey from the United Kingdom revealed that over 50% of adults take selfies (rising to 75% in the 18–24 age bracket) and that nearly half of this group upload these photographs to social media.⁶⁸ In the United States, a survey from August 2018 revealed that 62% of American adults take selfies.⁶⁹ Although few would consider selfies artwork, as photographs most selfies easily satisfy the statutory standard of creativity and would be protected by copyright.⁷⁰ Other social media users, such as hobbyists or professional artists, writers, photographers, musicians, and designers, use social media platforms to share their artwork.⁷¹ For these users, copyrights are especially important as a means to protect the integrity of their work.⁷²

When an original work of authorship meets the requirements of originality and fixation, the author of that work is granted six exclusive rights of ownership.⁷³ These rights include the right to reproduce the work, the right to prepare derivative works, the right to distribute copies of the work, the right to perform audiovisual works publicly, the right to perform sound recordings publicly, and the right to display the work publicly.⁷⁴ These rights are vested

67. See Alison C. Storella, *NOTE: It's Selfie-Evident: Spectrums of Alienability and Copyrighted Content on Social Media*, 94 B.U.L. REV. 2045, 2050 (2014) (providing statistics of selfie usage in the United Kingdom in recent years as an example of “[s]elfies have become a worldwide phenomenon”).

68. *Id.*

69. J. Clement, *Share of adults in the United States Who Have Ever Taken a Selfie as of August 2018*, STATISTA (Nov. 5, 2018), <https://www.statista.com/statistics/683933/us-adults-shared-selfie/> (last visited Feb. 25, 2020).

70. 17 U.S.C. § 102(a) (2012) (extending copyright protections to works of authorship “include[ing] . . . “pictorial, graphic, and sculptural works”); see also, Storella, *supra* note 67, at 2050 (analyzing the selfie phenomenon as a copyrightable subject matter).

71. See Liz Douthwaite, Robert J. Houghton & Richard Mortier, *How Relevant is Copyright to Online Artists? A Qualitative Study of Understandings, Coping Strategies, and Possible Solutions*, 21 FIRST MONDAY 5 (2016), <https://doi.org/10.5210/fm.v21i5.6107> (“Most webcomic creators rely on posting to social media to find and maintain a thriving audience”). In our study about 35% of respondents stated that they are gaining some value other than merely social value (i.e., financial or reputational) from uploading UGC. See *infra* Section III.C.2.b).

72. See Craighton Berman, *An Artist's Guide to Copyrights*, THE CREATIVE INDEPENDENT, <https://thecreativeindependent.com/guides/an-artists-guide-to-copyrights/> (last visited Oct 11, 2020) (“As an artist, it is essential for you to understand your rights in your creations, and what to do if you believe those rights have been violated.”); RightsLedger, *Copyright Basics for Content Creators*, MEDIUM (Apr. 15, 2019), <https://medium.com/rightsledger/copyright-basics-for-content-creators-968ade8a4cb> (last visited Oct 11, 2020) (“[C]opyright is important to every creator, and understanding the basics can help every artist protect their work and their income.”).

73. 17 U.S.C. § 201(a) (2012) (“[C]opyright in a work protected under this title vests initially in the author or authors of the work.”); see also, Babovic, *supra* note 16, at 151 (arguing that in many cases the user is indeed the copyright owner and mention possible exceptions).

74. 17 U.S.C. § 106 (2012).

automatically with the creator without a need for notice or registration.⁷⁵ Once the copyrighted work is uploaded to social media, however, these rights are immediately subjected to a broad copyright license as mandated by each platform's ToS.

C. STANDARD FORM CONTRACTS AND THE COPYRIGHT BOILERPLATE

Half a century ago, W. David Slawson estimated that 99% of all contractual obligations are imposed unilaterally by one contracting party on the other rather than deriving from balanced negotiation and mutually informed consent.⁷⁶ Since Slawson's estimation, the prevalence of non-negotiated and unilaterally imposed contracts has only increased.⁷⁷ Unilateral, non-negotiated contracts (also known as "form" contracts, "boilerplate" contracts, "fine-print," or "contracts of adhesion") are offered to consumers on a take-it-or-leave-it basis with no opportunity for conciliation.⁷⁸

While enforceable by default, form contracts are suspicious in the eyes of many jurists because they so bluntly diverge from the Platonic ideals of meaningful consent and freedom of (and from) contracts.⁷⁹ Indeed, numerous studies have confirmed that consumers rarely read, poorly understand, and are often overly optimistic about the content of form contracts.⁸⁰ As explored later in Part IV, even economists who usually put their faith in the ability of free markets to generate efficient contractual obligations agree that form contracts may sometimes be inefficient and include terms that are detrimental to consumers' welfare.⁸¹

By making form contracts more prevalent and far easier for consumers to ignore, the digital revolution substantially magnified the social concerns associated with lack of meaningful consent and salience of terms, as boilerplate

75. The Berne Convention Implementation Act of 1988 did away with the formalities that authors had to comply with under earlier acts in order to receive copyright protection. Berne Convention Implementation Act of 1988, Pub. L. No. 100-568, 102 Stat. 2853 (1988).

76. W. David Slawson, *Standard Form Contracts and Democratic Control of Lawmaking Power*, 84 HARV. L. REV. 529, 529 (1971).

77. Robert A. Hillman and Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 435 (2002) ("People encounter standard forms in most of their contractual endeavors . . . standard forms govern [many types of] contractual relationships."); *see also* Korobkin, *supra* note 25, at 1203 ("[N]early all commercial and consumer sales contracts are form driven.").

78. *See, e.g.*, Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1174, 1177 (1983); MARGARET JANE RADIN, *BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW* 9 (2012).

79. *See generally* RADIN, *supra* note 78; Slawson, *supra* note 76; Korobkin, *supra* note 25.

80. *See infra* Section III.A.

81. *See infra* notes 205-206 and accompanying text (discussing Korobkin's market failure theory).

contracts (and licenses and consumer agreements associated with digital life, generally) became more prevalent.⁸² Indeed, “digital form contracts” (also known as “clickwrap” or “shrinkwrap” agreements) have become an inseparable part of the modern economy—we sign them to access websites, use mobile applications, activate licensed software, and unlock various digital services.⁸³ Multiple studies investigating these contracts have found them to be overbroad and potentially unfair from a user’s perspective.⁸⁴

In the case of social media, users encounter digital form contracts when they first log into the service and check the “I Accept” box at the end of the platform’s lengthy ToS agreement. Under the ToS of most social media platforms, users are required to subject the copyrights in their uploaded creative content to a detailed licensing agreement.⁸⁵ While users usually retain ownership of their work under the terms of most social media platforms, these license agreements also give platforms very broad discretion to use their users’ content as they see fit.⁸⁶ Moreover, unless it is stated otherwise in the platforms’ ToS, these copyright licenses apply automatically whenever users

82. See Elazari Bar On, *supra* note 25, at 589 (discussing the heightened social concern with digital form contracts in the digital age). The digital revolution made form contracts more concerning from a social perspective by making them more prevalent and easier to ignore. At least in the privacy arena, as professor Zuboff explained, even if users were to read and fully understand the terms of many digital services, they cannot fully comprehend the consequences of their agreement. This is because users’ personal data, once aggregated and analyzed by the service provider, may unlock meaningful insights that users cannot anticipate in advance. See SHOSHANA ZUBOFF, WRITTEN TESTIMONY SUBMITTED TO THE INTERNATIONAL GRAND COMMITTEE ON BIG DATA, PRIVACY, AND DEMOCRACY, BIG DATA 6 (2019). <https://www.ourcommons.ca/Content/Committee/421/ETHI/Brief/BR10573725/br-external/ZuboffShoshana-e.pdf>. (arguing that while users prescribe to the legal text visible to them, they also unconsciously prescribe to another “shadow text” that is “the result of [the service provider’s] proprietary analyses of the first text.”).

83. Kevin W. Grierson, *Enforceability of “Clickwrap” or “Shrinkwrap” Agreements Common in Computer Software, Hardware, and Internet Transactions*, 106 A.L.R.5th 309, 317 n.1 (2003) (A click-wrap agreement is defined as “[an] agreement [that] appears when a user first installs computer software obtained from an online source or attempts to conduct an Internet transaction involving the agreement, and purports to condition further access to the software or transaction on the user’s consent to certain conditions there specified; the user ‘consents’ to these conditions by ‘clicking’ on a dialog box on the screen, which then proceeds with the remainder of the software installation or Internet transaction.”).

84. See *infra* Section III.A.

85. See *infra* Section III.B.2.

86. See *infra* Section III.B.2; see also Babovic, *supra* note 16, at 160 (“Terms of service agreements, in general, license a significant chunk of exclusive rights associated with copyright, and have vague limitations on such a license.”); Gutierrez Alm, *supra* note 49, at 115 (“According to the [ToS], there is nothing stopping social media companies from selling copies of a user-photographer’s photos, for example, or placing them in advertisements.”); Allen & Ward, *supra* note 1, at 50–53 (reviewing ToS of Facebook, LinkedIn, Second Life, and Twitter).

upload a photo, share a video, or tweet a poem. The next Part introduces our study, which we designed to uncover the true breadth of these contractual licensing agreements, shed light on users' awareness, understanding, and expectations of these agreements, and to assess the salience of terms to the users.

III. THE STUDY

A. OBJECTIVES AND RELATED WORK

Studies have established that digital form contract terms are notoriously lengthy,⁸⁷ complex,⁸⁸ rarely read,⁸⁹ hardly understood,⁹⁰ and often perceived by consumers to be more favorable than they actually are.⁹¹ As the notion of *term*

87. See Aaron Perzanowski & Chris Jay Hoofnagle, *What We Buy When We Buy Now*, 165 PEN L. REV. 315, 320 (2017) (citing Tom Gardner, *To Read, or Not to Read . . . the Terms and Conditions*, DAILY MAIL (Mar. 22, 2012), <http://www.dailymail.co.uk/news/article-2118688/PayPal-agreement-longer-HamletiTunes-beats-Macbeth.html>) (noting that iTunes's ToS are longer than Shakespeare's Macbeth).

88. See DOUGLAS E. PHILLIPS, *THE SOFTWARE LICENSE UNVEILED: HOW LEGISLATION BY LICENSE CONTROLS SOFTWARE ACCESS* 79 (2009) (using the Flesch-Kincaid readability formula to analyze an Adobe licensing agreement and finding that a reader would likely need at least 19.3 years of formal education in order to decipher it); see also Carlos Jensen & Colin Potts, *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*, 2004 PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 471, 473–75.

89. Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts*, 43 J. LEGAL STUD. 1, 1(2014) (finding that users access software retailers' End-User Licensing Agreements (EULA) only 0.05% of the time); see also Nathaniel Good, Jens Grossklags, Deirdre K. Mulligan & Joseph A. Konstan, *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 607, 611 (finding that less than 2% of users reported reading EULAs thoroughly with about two thirds saying that they did not read them at all); Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts"*, 78 U. CHI. L. REV. 165, 179–81 (2011) (reporting empirical data supporting the conclusion that license terms "are almost always ignored"); Rainer Böhme & Stefan Köpsell, *Trained to Accept? A Field Experiment on Consent Dialogs*, 2010 PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 2406 (showing that most users take less than 8 seconds to click through a consent dialog).

90. See Joel R. Reidenberg, Travis Breaux, Lorrie F. Cranor, & Brian M. French, *Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39 (2015) (asking comprehension questions about privacy policies to non-expert users, knowledgeable users, and privacy experts, finding discrepancies between non-expert users and experts (and even among experts), and concluding that websites do not convey information in a way that is accessible to reasonable users).

91. Ayres & Schwartz, *supra* note 29, at 551 (arguing that consumers often "expect a contract to contain more favorable terms than it actually provides"). Professors Aaron

salience emerged as a primary scrutinizing factor in the context of form contracts more generally, privacy scholars have also looked at the question of privacy's salience, defined by the degree to which privacy's prominence in people's awareness actually impacts their real-world privacy decisions.⁹²

In this vein, multiple scholars have pointed out a “privacy paradox” in which users who claim to care about privacy policies often behave inconsistently with their stated pro-privacy preferences. One study, for example, found that users who mentioned that they feel strongly about not sharing their contacts' information were happily willing to do just that moments later when offered a free pizza slice in exchange for their friends' email addresses.⁹³ Another study confirmed that users shared nearly twice as much personal information compared to what they initially stated they were willing to share.⁹⁴

Unlike in the privacy arena, almost no studies have looked at users' awareness, perceptions, expectations or overall term salience regarding platforms' UGC licensing policies. Several legal scholars, apparently motivated by empirical evidence in the privacy sphere, have speculated that users are unlikely to read or understand UGC licensing provisions⁹⁵ or comprehend the

Perzanowski & Chris Jay Hoofnagle have recently documented such false “term optimism” in the context of e-commerce by showing that consumers tend to overestimate the rights that they acquire when they press the “Buy Now” buttons that appear in such websites. Perzanowski & Hoofnagle, *supra* note 87; see also Nathaniel Good & Joseph A. Konstan, *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, 2005 PROCEEDINGS OF SYMPOSIUM ON USABLE PRIVACY AND SECURITY (SOUPS) 43, 43 (finding that there is a “strong disconnect” between their actual content and users' expectations); see also Aaron Perzanowski & Jason Schultz, *Reconciling Intellectual and Personal Property*, 90 NOTRE DAME L. REV. 1211, 1257 (2015) (noting the potential for consumer misunderstanding as a result of the *Buy Now* button).

92. See Meredydd Williams, Jason R. C. Nurse & Sadie Creese, *Privacy Salience: Taxonomies and Research Opportunities*, IFIP INTL. SUMMER SCH. ON PRIVACY & IDENTITY MGMT., 263, 263–78 (summarizing research and defining privacy salience “as whether an individual is currently considering the topic of informational privacy”).

93. Susan Athey, Christian Catalini & Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, MIT SLOAN RESEARCH PAPER NO. W23488 (2017), https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141392.pdf.

94. Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, 41 J. CONSUMER AFF. 100, 118 (2007).

95. See Gutierrez Alm, *supra* note 49, at 114 (“The majority of users would likely be surprised to learn that they have licensed such broad latitude with their user-generated content.”); Kelly, *supra* note 7, at 515 (“[U]sers are bound by terms they do not understand, with little recourse and seemingly endless policing of the contractual boundaries by Internet conglomerates.”); see also, Alina Tugend, *Those Wordy Contracts We All So Quickly Accept*, N.Y. TIMES (July 12, 2013), <https://www.nytimes.com/2013/07/13/your-money/novel-length-contracts-online-and-what-they-say.html>. <https://perma.cc/K2AJ-GDEY>.)

legal rights they have in the digital sphere.⁹⁶ Several studies have confirmed these views by showing, for example, that the ToS of some social media platforms are difficult to read⁹⁷ and that users often misunderstand how copyright law operates in the online environment, particularly since subjective concepts such as fair use are relevant in this context.⁹⁸

Only a handful of studies, however, have poked into users' expectations of UGC licensing policies and evaluated the subjective salience of various terms. And those that did drew incoherent results. For example, professors Casey Fiesler, Cliff Lampe, and Amy Bruckman investigated users' perceptions of UGC licensing policies across various websites (including some social media

96. See Storella, *supra* note 67, at 2045 (“[T]he majority of social media users are likely unaware that copyright protection extends to their posted materials at all.”); Kelly, *supra* note 7, at 514 (“Many users may not realize that the content they post on social media platforms is copyrighted, and so will not fully understand the license they are granting.”). This view was bolstered by the notion that many social platforms, while vigorously discussing copyright in their ToS, do very little to educate users about what copyright *is*. For instance, by giving examples of copyrighted material. See, e.g., Gard & Whetstone, *supra* note 28, at 269 (“Pinterest and others engaged in a copyrighted world protect themselves from legal harm, while not educating or advising their users of how copyright works within their system.”).

97. On the issue of readability, see Casey Fiesler, Cliff Lampe & Amy S. Bruckman, *Reality and Perception of Copyright Terms of Service for Online Content Creation*, 2016 PROCEEDINGS OF THE 19TH ACM CONFERENCE ON COMPUT. SUPPORTED COOPERATIVE WORK & SOC. COMPUT. (showing that the average Flesch-Kincaid Grade Level Score of many copyright terms was a college sophomore reading level of 14.8 (in a range of 8.4 to 19.8); see also, Amy B. Wang, *A Lawyer Rewrote Instagram's Terms of Use 'In Plain English' So Kids Would Know Their Privacy Rights*, WASH. POST (Jan. 8, 2017), <https://www.washingtonpost.com/news/parenting/wp/2017/01/08/a-lawyer-rewrote-instagram-terms-of-use-in-plain-english-so-kids-would-know-their-privacy-rights/> (showing that at the time of the study, Instagram's ToS required a postgraduate level of reading comprehension); Kelly, *supra* note 7, at 515 (“[M]ost adults do not have the requisite postgraduate degree apparently required to understand the terms and conditions that they are contractually binding themselves to obey.”); 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’N & SOC. 1, 16 (finding that the 543 participants who joined the study's fictitious social network had spent 51 seconds on average reading the website's ToS, with a 93% acceptance rate).

98. Fair use, perhaps the most complex copyright doctrine to analyze, is an affirmative defense against the claim of copyright infringement. Evaluating whether a work is fair use (and therefore not infringing) requires a delicate balancing of four statutory factors: the purpose of the intended use, the nature of the copyrighted work, the amount and substantiality of the portion used of the copyrighted work, and the effect of the use on the copyrighted work's market. 17 U.S.C. § 107 (1992); see also Casey Fiesler & Amy S. Bruckman, *Remixers' Understandings of Fair Use Online*, 2014 PROCEEDINGS OF THE ACM CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK & SOCIAL COMPUTING 1023; Casey Fiesler, Jessica Feuston & Amy S. Bruckman, *Understanding Copyright Law in Online Creative Communities*, 2015 PROCEEDINGS OF THE ACM CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK & SOCIAL COMPUTING 116; Catherine C. Marshall & Frank M. Shipman, *The Ownership and Rense of Visual Media*, 2011 PROCEEDINGS OF THE 11TH ACM/IEEE-CS JOINT CONFERENCE ON DIGITAL LIBRARIES 157.

platforms), finding that “users care about how their content can be used yet lack critical information.”⁹⁹ The researchers did not inquire about the salience of copyright terms to users—namely whether users would change their online uploading behavior if they were given more information (although they speculated that this might be the case).¹⁰⁰

Conversely, in another study, professors Liz Dowthwaite, Robert Houghton, and Richard Mortier asked for the perceptions of professional webcomic artists and concluded that such users are somewhat agnostic about copyright policies (including UGC licensing terms) and often rely on one another to red flag substantial concerns.¹⁰¹ These findings suggest that better information about UGC licensing policies is unlikely to change users’ social media behavior.¹⁰²

Finally, commenters also seem to disagree as to whether and to what extent copyright ToS provisions vary across social media platforms. While some commenters argue that copyright provisions are all boilerplate terms,¹⁰³ others suggest that there is a great deal of term variability between different websites.¹⁰⁴ Our study fills these gaps—it is the first study to check the conformity of UGC policies among the most popular social media platforms and to appraise the saliency of these policies to users.¹⁰⁵ The study includes two parts. The first part—a comparative textual analysis of platforms’ ToS—is discussed next. The second part—a survey of users’ awareness, understanding, and expectations and of terms’ salience—is discussed in Section III.C.

99. See Fiesler et al., *supra* note 97, at 1453.

100. See *id.* at 1458 (“[W]e did not ask our participants directly about how licensing terms would affect their site use.”).

101. See Dowthwaite et al., *supra* note 71 (“Creators also tended to rely on each other to point out any issues: ‘I think my feeling is always like well everyone else seems to be using it so I’m sure it’s fine.’”).

102. See, e.g., Babovic, *supra* note 16, at 191 (“It might be said that many users would be willing to surrender their control over UGC that they submit; that it is understood as a price to be paid in order to participate in social media and social networking generally.”).

103. See, e.g., Storella *supra* note 67 at 2064 (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”).

104. See Fiesler et al., *supra* note 97, at 1458 (“[C]opyright licenses are far from one size fits all . . . This goes against conventional wisdom that the legalese in TOS is all boilerplate terms.”).

105. Cf. Fiesler et al., *supra* note 97 (investigating only eight social media platforms within a broader dataset of thirty websites and not investigating salience); Dowthwaite et al., *supra* note 71 (investigating users’ perceptions of copyright policies but focusing on the small subset of users who are professional creators).

B. MAPPING THE COPYRIGHT BOILERPLATE LANDSCAPE

1. *Methods*

To evaluate whether and to what extent the terms that govern UGC vary across different platforms, we have conducted a textual analysis of the ToS of eleven leading social media and content-sharing platforms: Facebook, YouTube, Instagram, Twitter, Pinterest, Snapchat, LinkedIn, Reddit, Vimeo, Vine, and Tumblr. The first eight platforms in our dataset were considered by most measures to be among the ten most popular social media platforms in Western societies (excluding chat-only platforms such as WhatsApp and Skype), amounting to around 80% of active social media users.¹⁰⁶ We also included Vimeo, Vine, and Tumblr due to the substantial amount of copyrighted UGC shared on these platforms and their popularity among advertisers.¹⁰⁷ Our sample is thus representative of the most commonly used social media platforms for UGC sharing and a number of additional platforms for content sharing.¹⁰⁸

We analyzed the ToS provisions of these platforms as of March 1, 2018. We have further confirmed that the relevant terms remain materially (for the purpose of the survey) the same as of February 2020, following the collection of survey answers.¹⁰⁹ Based on our analysis, we identified and characterized seven key elements that reflect ToS terms concerning copyrightability and other related aspects of UGC. We offer the following taxonomy:

106. Irfan Ahmad, *The Most Popular Social Media Platforms of 2019*, DIGITAL INFORMATION WORLD (Jan. 1, 2019) <https://www.digitalinformationworld.com/2019/01/most-popular-global-social-networks-apps-infographic.html> (last visited Feb. 25, 2020); Andrew Perrin & Monica Anderson, *Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018*, PEW RESEARCH CENTER, <https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/> (last visited Feb. 25, 2020); see also Alexa top 500, “online communities,” https://www.alexa.com/topsites/category/Top/Computers/Internet/On_the_Web/Online_Communities/Social_Networking (listing between 1 to 4, Facebook, Twitter, LinkedIn and Pinterest); eBizMBA, *Top 15 Best Web 2.0 Websites | February 2020*, <http://www.ebizmba.com/articles/web-2.0-websites> (last visited Feb. 25, 2020) (ranking among the top 15 Web 2.0 websites (at the time): YouTube, Twitter, Pinterest, and Tumblr and Instagram).

107. See, e.g., Mediakix, *Have We Seen The End Of Vine?*, <https://mediakix.com/blog/vine-app-losing-popularity/> (last visited Feb. 25, 2020). Notably, the popularity of Vine for advertising purposes is reportedly decreasing. See Lauren Johnson, *Why Brands Are Ditching Twitter’s 6-Second Vine App*, ADWEEK (Dec. 6, 2015), <https://www.adweek.com/digital/why-brands-are-ditching-twitter-s-6-second-vine-app-168433/> (last visited Feb. 25, 2020).

108. Although the boilerplate landscape mapping included Tumblr in the survey, we omitted survey questions related to this platform since there was no adequate sample of Tumblr users.

109. Some updates in the platforms’ ToS following our survey from this analysis are summarized in the footnotes of Appendix A.

1. **Perpetuity:** Language regarding the persistence of copyright licenses to the UGC even after the user-platform agreement has terminated.
2. **Third parties:** Language referring to the platform's ability to sublicense or otherwise permit third parties (such as affiliated businesses) to use the copyrighted work in different ways (e.g., to publish or display the work).
3. **Modification:** Language about the platform's ability to change or modify the copyrighted work.
4. **Derivative works:** Language regarding the platform's ability to create derivative works defined under 17 U.S.C. § 101.¹¹⁰
5. **Immediate Removal:** Language providing the platform the ultimate discretion to unilaterally remove UGC from its service.
6. **Commercial:** Language addressing the platform's ability to utilize UGC for commercial purposes (such as advertising).¹¹¹
7. **Other:** Language addressing the following issues:
 - a) **Moral Rights:** Language specifically requiring users to disclaim moral rights (a term commonly known to include the right for attribution and integrity as defined by 17 U.S.C. § 101).¹¹²

110. "A 'derivative work' is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship, is a 'derivative work.'" 17 U.S.C. § 101.

111. Some platforms use broader language to enable unlimited commercial uses, other platforms limit their ability to commercialize UGC to promoting their services. For a detailed comparative analysis of the platforms' terms, see Appendix A.

112. Attribution includes the right "to claim authorship of [the] work." 17 U.S.C. § 106A(a)(1)(A). Integrity includes the right "to prevent any intentional distortion, mutilation, or other modification of that work which would be prejudicial to [the creator's] honor. . . ." 17 U.S.C. § 106A(a)(3)(A). As explained, U.S. law does not recognize moral rights for UGC. *See supra* note 7. Accordingly, specific waiver of moral rights in the platforms' ToS has no practical meaning. Nevertheless, we still considered the issue of moral rights because we suspected that users care very deeply about those rights, especially the right for attribution. (Our survey later substantiated this suspicion). *See infra* Section III.C.2.c).

- b) **Publicity Rights:** Language regarding instances where platforms specifically claim the right to use users' identity (i.e., name, likeness, and voice).¹¹³
- c) **Ideas:** Language specifically requiring users to waive any claim to compensation or liability with respect to ideas they provide the platform.

We intentionally disregarded elements that are essential for the platforms' operation or functionality, such as having the right to display or distribute UGC.¹¹⁴ Instead, we focused our attention on elements that either provide platforms with substantial control over users' content (such as the right to modify) or that can significantly undermine artistic values and interests (such as denying attribution or subjecting the work to advertising).¹¹⁵ We manually compared the ToS of each platform in our dataset to evaluate how the stated elements conformed or differed across platforms. We considered that a platform has a stated element only if its ToS stated the element explicitly and unmistakably based on the taxonomy we have proposed above. For example, Reddit's ToS addresses four of the seven key elements in a single, concise provision (the number in brackets corresponds with the element's number as it appears in the list above):

“By submitting user content to Reddit, [users] grant [Reddit] a royalty-free, perpetual [1], irrevocable [1], non-exclusive, unrestricted, worldwide license to reproduce, prepare derivative works [4], distribute copies, perform, or publicly display your user content in any medium and for any purpose, including commercial purposes [6], and to authorize others to do so [2].”¹¹⁶

A summary of our textual analysis appears in Figure 1 (the complete table of the investigated terms broken down by key elements appears in Appendix

113. Publicity rights protect against the misrepresentation of one's name, voice, or likeness. *See, e.g.*, Cal. Civ. Code § 3344 (2000) (“Any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner. . . without such person's prior consent. . . shall be liable for any damages sustained by the person. . .”). For a discussion of the right of publicity and the challenges imposed on it by social platforms see Jesse Koehler, *Fralely v. Facebook: The Right of Publicity in Online Social Networks*, 28 BERKELEY. TECH. L. J. 963 (2013).

114. *See* Fiesler et al., *supra* note 97, at 1454 (“When a user submits content to one of these websites, they are typically licensing that work for use by the site—at the very least, the site must be permitted to display the work, or others would not be able to see it.”). However, we did address the right to display and distribute as means to investigate other related issues—for instance, the platforms' ability to sublicense these rights or to exercise them outside the platforms' services. *See infra* Section III.C.1.c).

115. In this respect our approach is normative rather than pragmatic (as explained, U.S. law does not recognize moral rights for UGC.). *See supra* note 7.

116. *See* Reddit, *supra* note 4.

A). In addition to our comparative similarity analysis, we also gathered statistical text information and evaluated the terms' readability. A discussion of our findings follows.

2. Findings

a) Terms' Readability

We tested the terms that govern UGC for readability using the Flesch-Kincaid Grading System, which was commonly used in similar studies dealing with privacy policies.¹¹⁷ The average Flesch-Kincaid Grade Level Score (representing a U.S. educational grade level) for the UGC terms in our dataset was in a postgraduate reading comprehension level of 17.4. The scores ranged from 13.4 to 27.4 (see Figure 1). These results are significantly higher than the findings of most comparable studies in the privacy realm (which are usually in the range of 14 to 15).¹¹⁸ As the results indicate, many users would find it extremely challenging to understand the legal terms contained in social media platforms' ToS.¹¹⁹

It is difficult to justify these terms' linguistic complexity. Unlike other elements in the ToS agreement that are arguably inherently complex—such as the Digital Millennium Copyright Act (DMCA) takedown procedure¹²⁰—the UGC licenses platforms require to operate their services are relatively

117. See Fiesler et al., *supra* note 97, at 1453; see also, Mary J. Culnan & Thomas J. Carlin, *Online Privacy Practices in Higher Education: Making the Grade?*, 52 COMMUNICATIONS OF THE ACM 2, 126–130 (March 2009); Mark A. Graber, Donna M. D'Alessandro & Jill Johnson-West, *Reading Level of Privacy Policies on Internet Health Web Sites*, 51 THE JOURNAL OF FAMILY PRACTICE 7, 642–45 (2002); Jensen & Potts, *supra* note 88 at 473–75.

118. See, e.g., Jensen & Potts, *supra* note 88 at 473–75; Mark A. Graber, Donna M. D'Alessandro & Jill Johnson-West, *Reading Level of Privacy Policies on Internet Health Web Sites*, 51 J. OF FAM. PRAC. 7, at 642–45 (2002); see also Fiesler et al., *supra* note 97, at 1453 (finding an average of 14.8 for UGC policies across the web).

119. See U.S. Social Reach by Education 2019, STATISTA, <https://www.statista.com/statistics/471386/us-adults-who-use-social-networks-education/> (last visited Oct 10, 2020) (noting, for example, that 64% of adults whose educational background was high school grad or less were using social networks). This concern is especially noteworthy with respect to platforms that are popular among teens and children such as Instagram. See, e.g., Wang, *supra* note 97 (noting that simplifying ToS is important for all platforms but it is more critical for Instagram “for its ubiquity and popularity among teenagers”).

120. The DMCA's notice and take down regime requires content-sharing platforms to remove copyright infringing content upon the copyright owner's notice. 17 U.S.C. § 512 (c)(1)(A)(1998). This procedure is often described as complex and confusing. See, e.g., Micah Singleton & Ben Popper, *The Music Industry Cranks Up the Volume In Its Fight Against YouTube*, THE VERGE (2016), <https://www.theverge.com/2016/6/3/11852146/music-industry-fighting-youtube-dmca> (last visited Oct 11, 2020) (“The industry's biggest complaint about the DMCA is that the take-down process for unlicensed content is too complicated . . .”).

straightforward. Little prevents platforms from simplifying the obscure legalese in these terms and clearly communicating how they will use UGC.

Interestingly, while providing users with such additional clarity should not be overly challenging or costly to platforms, only three platforms in our dataset—Pinterest, Tumblr, and LinkedIn—have included a shortened and simplified version of their main terms in plain English.¹²¹ As seen in Figure 1 below, the average Flesch-Kincaid Grade Level Score of these simplified terms was 8.77, which is on par with children’s novels.¹²² Another useful way platforms can simplify their ToS is to use instructional videos just as LinkedIn did back in 2014.¹²³ We further discuss the benefits of simplified disclosures in Section IV.A.¹²⁴

b) Similarity and Breadth of User-Generated Content Licensing Terms

As depicted in Figure 1, our findings point to a substantial similarity in the platforms’ approaches in our dataset with respect to the seven key elements. All the platforms, for example, required the right to assign and sublicense UGC rights to third parties such as affiliated businesses. Most platforms also required users to provide them with the right to modify content, to create derivative works, or both. Moreover, as seen in the complete textual analysis in Appendix A, many phrases used by social media platforms in their UGC provisions have minimal variability.¹²⁵ This finding confirms the view that legalese in ToS appears in a boilerplate form.¹²⁶

121. See Pinterest, *Terms of Service*, <https://policy.pinterest.com/en/terms-of-service> (last visited Sept. 24, 2021); Tumblr, *Terms of Service*, (July 21, 2021), <https://www.tumblr.com/policy/en/terms-of-service>; LinkedIn, *User Agreement*, (Aug. 11, 2020), <https://www.linkedin.com/legal/user-agreement>.

122. See *The Flesch Reading Ease and Flesch-Kincaid Grade Level*, READABLE, <https://readable.com/blog/the-flesch-reading-ease-and-flesch-kincaid-grade-level/> (last visited Feb. 11, 2020).

123. *LinkedIn User Agreement | Who owns your content? You do*, https://www.youtube.com/watch?v=ha7ASaPnjbA&feature=emb_title (last visited Feb. 11, 2020).

124. See *infra* notes 235–237 and accompanying text.

125. See *infra* Appendix A. For example, compare the following excerpts from our study’s platforms: “[Y]ou grant us [Twitter] a worldwide, non-exclusive, royalty-free license”; “You grant Pinterest and our users a non-exclusive, royalty-free, transferable, sublicenseable, worldwide license”; “[Y]ou hereby grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license”; “[Y]ou grant us [Facebook] a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license”; “[Y]ou grant YouTube a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license”; “[Y]ou grant Vimeo and its affiliates a limited, worldwide, non-exclusive, royalty-free license.”

126. But see Fiesler et al., *supra* note 97, at 1458 (“Based on our analysis of what terms exist on different websites, we see a great deal of variability This goes against conventional wisdom that the legalese in TOS is all boilerplate terms.”)

More substantially, our findings affirm the concerns that were often raised in the privacy arena—that boilerplate terms in digital form contracts are grossly and perhaps unjustifiably overbroad.¹²⁷ Many of the UGC licenses in our dataset used the following legal terminology (in brackets is the number of times these words appear in our ToS dataset)¹²⁸: “perpetual” [1], “irrevocable” [2], “sublicensable” [5], “nonexclusive” [12], “royalty-free” [11], “transferable” [7], “unrestricted” [3], and “worldwide” [4]. These ToS also had language that enabled platforms, among other things, to modify [14], adapt [10], edit [4], and improve [3] UGC; to create derivative works [10]; and to commercially exploit their users’ content.¹²⁹

127. *See infra* Section III.A (giving the example that platforms obtain a broad copyright license for “any commercial license”).

128. *See infra* Appendix A.

129. Of all the platforms in our dataset, Reddit’s ToS contained the broadest language concerning discretion to commercial UGC. *See* Reddit, *supra* note 4. Since conducting our study, Reddit has narrowed its provision and this language was removed. Reddit, *supra* note 7.

Figure 1: Textual Analysis of Platforms' UGC Terms

| | | F-K | Perpetuity | Third parties | Modification | Derivative works | Immediate removal | Commercial | Other | | |
|----|-----------------------------|-------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | | | | | | | | Moral rights | Publication rights | Ideas |
| 1 | Facebook | 13.8 | <input type="checkbox"/> | | | |
| 2 | YouTube | 18.7 | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | |
| 3 | Instagram | 17.8 | | <input type="checkbox"/> | | | |
| 4 | Twitter | 15.7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> | | | <input type="checkbox"/> |
| 5 | Pinterest | 16.5 / 7.1 | <input type="checkbox"/> | | | | <input type="checkbox"/> |
| 6 | Snapchat | 13.4 | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | LinkedIn | 12.3 / 8.9 | | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> | | | <input type="checkbox"/> |
| 8 | Reddit | 27.4 | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | |
| 9 | Vimeo | 14.0 | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> |
| 10 | Vine | 18.7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> | | | |
| 11 | Tumblr¹³⁰ | 23.7 / 10.3 | <input type="checkbox"/> | | | |

Arguably, policymakers should not be bothered by the fact that the UGC licensing policies are overbroad because platforms are unlikely to fully exhaust

130. Although at the time of the study Tumblr has claimed a relatively broad UGC license, they also subsequently added limiting language that substantially narrowed their discretion to misuse users' content. *See infra* note 237.

their legal privileges in fear of awakening the wrath of the public.¹³¹ Although this argument is not without merit, overbroad UGC licensing policies are concerning for at least two reasons. First, while it is indeed unlikely that platforms “sublicense user content to porno.com,”¹³² it is conceivable that platforms could come up with creative new ways to monetize their users’ content without creating an immediate backlash.¹³³ This possibility is especially valid at the present moment as growing political and public pressure is causing platforms to lose revenue from monetizing users’ data (the platforms’ primary source of income), incentivizing platforms to rethink their monetization

131. Indeed, platforms zealously defend their public image, especially when facing a potential public relationship crisis. *See infra* notes 229–230 and accompanying text; *see also* Craig Silverman, Ryan Mac & Pranav Dixit, “I Have Blood On My Hands”: A Whistleblower Says Facebook Ignored Global Political Manipulation, BUZZFEED NEWS, <https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo> (last visited Oct 11, 2020) (discussing how a former Facebook employee is accusing the platform of prioritizing potential public-relation concerns in Western democracies but not expressing the same concern for malign activities in other regions where the possibility of journalistic coverage leading to public outcry is less likely).

132. Hetcher, *supra* note 9, at 848 (noting that Facebook could “surreptitiously sublicense user content to porno.com . . . [which] would fall squarely within the license Facebook purports to be granted by users”).

133. *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 235, 235 (Oxford, 2019) (arguing that “[t]he increasingly indispensable nature of the services that platforms provide makes exits particularly infeasible for many users”); *see also* Mireille Hildebrandt, *Primitives of Legal Protection in The Era of Data-Driven Platforms*, 2 GEO. L. TECH. REV. 252, 254 (2018) (“Even if a platform does not intend to use its quasi-sovereign powers to actually institute a quasi-totalitarian rule across the many contexts we navigate, we should be concerned about its potential to do so.”); Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, GEO. L. TECH. REV. 275, 295 (2018) (“A second way data-opolies can extract wealth is by getting creative content from users for free.”). As a cautionary tale, consider the recent case in which the Federal Trade Commission “investigated allegations that Google unfairly ‘scraped,’ or misappropriated [others’] content (including of artists), . . . passed this content off as its own, and then threatened to delist these rivals entirely from Google’s search results when they protested the misappropriation of their content.” Statement of the U.S. Federal Trade Commission Regarding Google’s Search Practices, *In the Matter of Google, Inc.*, FTC File No. 111-0163, at 3, n.2 (Jan. 3, 2013), https://www.ftc.gov/system/files/documents/public_statements/295971/130103googlesearchstmtofcomm.pdf. As one complainant noted, “Artists need to earn a living in order to sustain creativity and licensing is paramount to this; however, this cannot happen if Google is siphoning traffic and creating an environment where it can claim the profits from individuals’ creations as its own.” Samuel Gibbs, *Getty Images Files Antitrust Complaint Against Google*, GUARDIAN (Apr. 27, 2016), <https://www.theguardian.com/technology/2016/apr/27/getty-imagesfiles-antitrust-google> [<https://perma.cc/5WZK-EF98>]. This case settled in 2018. Chris O’Brien, *Getty Images and Google Declare a Truce with New Image Licensing Partnership*, VENTURE BEAT (Feb. 9, 2018), <https://venturebeat.com/2018/02/09/getty-images-and-google-declare-a-truce-with-newimage-licensing-partnership/> [<https://perma.cc/A4LD-FGH3>].

practices.¹³⁴ Indeed, as Angel Fraley’s (sponsored) story from the introduction indicates, social media platforms will not shy away from promising new avenues for generating income.¹³⁵

The second and main reason to be concerned about platforms’ overbroad discretion to exploit UGC is that—as indicated by our survey findings below—users do not actually know and do not expect that platforms have such discretion.¹³⁶ Moreover, most users even claim that they would change their uploading behavior to social media if they knew how much discretion social media platforms have in manipulating their UGC.¹³⁷ Thus, overbroad UGC licenses raise social concerns from both copyright and contract law perspectives.¹³⁸

C. USERS’ AWARENESS, UNDERSTANDING, AND EXPECTATIONS AND TERMS’ SALIENCE SURVEY

1. *Methods*

Our initial survey pool consisted of 1,100 respondents (N=1,100) from Mechanical Turk.¹³⁹ The respondents were generally representative of the U.S. social media adult population.¹⁴⁰ Our survey opened with a screening question designed to filter only those social media users who reported uploading creative content to at least one of the survey’s participating platforms.¹⁴¹ Users who did not upload content did not complete the survey. We then asked respondents a series of demographic questions, including gender, age,

134. See generally Zuboff, *supra* note 19 (noting that the business model of most social media platforms is based on targeted advertising, which is fueled by and thrives on users’ data). Mark Zuckerberg famously said to Senator Orrin Hatch, “Senator, we run ads,” a statement that became a well-known meme. See Emily Stewart, *Lawmakers Seem Confused About What Facebook Does—and How to Fix It*, VOX (Apr. 10, 2018), <https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations>.

135. A class action, brought against Facebook for its attempt to commercialize users’ stories, settled for 20 million dollars in 2013. See *supra* note 10. According to the filings in the case, Facebook allegedly charged advertisers 234 million dollars for “Sponsored Stories” between January 2011 and August 2012. Dan Levine, *U.S. judge approves Facebook privacy settlement over ads*, REUTERS (Aug. 26, 2013), <https://www.reuters.com/article/net-us-facebook-privacy-settlement/u-s-judge-approves-facebook-privacy-settlement-over-ads-idUSBRE97P0VG20130826>.

136. See *infra* Section III.C.2.c), III.C.2.d).

137. See *infra* Section III.C.2.e); see also Fiesler et al., *supra* note 97 (“Many users are granting these rights without realizing, and they might be unhappy if they knew.”).

138. See *infra* notes 240–245 and accompanying text.

139. Amazon Mechanical Turk is a popular crowdsourcing marketplace tool used, among other things, to source experimental data and conduct surveys and empirical research. See Amazon, *Amazon Mechanical Turk*, <https://www.mturk.com/>.

140. See *infra* Section III.C.2.a (Figure 6).

141. See *infra* Appendix B (Survey Section 2).

education, and income.¹⁴² Figure 6, below, shows a sample of the respondents' demographic information.

The final preliminary step required respondents to review a brief definition page that introduced, in layperson's terms, four legal concepts contained in the survey: (1) "Work or Content," (2) "Platform or Social Media Platform," (3) "Use," and (4) "Term."¹⁴³ We defined the term "Work or Content" to mean those copyright-protected materials created and uploaded by the user, including art, poetry, prose, photographs, sound and musical compositions, illustrations, video, or audiovisual works.¹⁴⁴ "Platform or Social Media Platform" denoted the ten platforms that we chose to survey: Facebook, Instagram, YouTube, Twitter, Snapchat, LinkedIn, Vimeo, Reddit, Pinterest, and Vine.¹⁴⁵ "Use" meant to publicly display, copy, reproduce, distribute, perform, or transmit the work.¹⁴⁶ Finally, "Terms" denoted the platforms' terms of use or the contract that required the users to click "I Accept" when they joined the platform.¹⁴⁷

The substantive portion of the survey was organized around four sets of questions: (1) *Social Media Usage* (asking how frequently respondents uploaded content to social media and what value they derived from doing so),¹⁴⁸ (2) *Awareness and Understanding* (asking respondents to identify, to the best of their knowledge, the legal terms included in the platforms' ToS and their meanings¹⁴⁹); (3) *Expectations* (asking what respondents thought the UGC licensing terms in the platforms' ToS should be),¹⁵⁰ and, finally, (4) *Salience* (asking respondents how likely they would be to change their social media uploading patterns once they understood the legal terms in the platforms' ToS).¹⁵¹

a) Social Media Usage

We asked respondents to indicate how frequently they upload content to social media, as well as what kind of value (if any) they derive from doing so. Concerning value obtained, we asked respondents (1) whether they receive direct income from uploading content; (2) whether they do it for other

142. See *infra* Appendix B (Survey Section 3).

143. See *infra* Appendix B (Survey Section 4).

144. *Id.*

145. *Id.*

146. *Id.*

147. *Id.*

148. See *infra* Appendix B (Survey Section 5).

149. See *infra* Appendix B (Survey Section 8).

150. See *infra* Appendix B (Survey Section 7).

151. See *infra* Appendix B (Survey Section 9).

promotional reasons (self or business); (3) whether they do it to increase awareness of their work (“getting the work out there”); or (4) whether their only gain is social interaction.¹⁵² As to frequency, we inquired whether users upload their UGC to social media platforms once (or more) a day, once a week, once a month, or once every couple of months.¹⁵³ Finally, we asked respondents to indicate to which of the platforms in our dataset they upload their content.¹⁵⁴ Figures 7 through 8 in Section III.C.2.b summarize these social media usage patterns.

We categorized our respondents’ answers to these questions to determine whether and to what extent our findings would vary across the different categories. Common sense would suggest, for example, that users who use social media platforms more frequently or who are financially and reputationally dependent on these platforms would also be more term conscious.¹⁵⁵ Previous studies have ignored this distinction or looked only at a single group of social media users (either amateurs or professionals), which prevented researchers from taking a comparative approach like ours.¹⁵⁶

b) Awareness and Understanding

This portion of the survey extended privacy scholars’ work on user awareness and understanding of UGC licensing policies.¹⁵⁷ To achieve this goal, we first classified respondents based on uploading habits—that is, we only asked users who reported that they upload content to a platform about the applicable terms of *that* platform. We presented respondents with a series of affirmative statements and asked whether those statements were correct according to the platform’s ToS. Respondents could mark each statement as correct or incorrect, or respondents could indicate they did not know the

152. See *infra* Appendix B (Survey Section 5, questions 1–2).

153. See *infra* Appendix B (Survey Section 5, question 3).

154. See *infra* Appendix B (Survey Section 6, question 1).

155. Compare with Dowthwaite et al., *supra* note 71, who observed that user-creators tend to rely on their community for flagging any copyright concerns with respect to their UGC. One user-creator, for example, was quoted saying that “watchdogs keep me informed. Artist communities are good at trading this kind of information and flagging up any incidents that other artists need to watch out for.” *Id.* Somewhat surprisingly, our findings did not support a conclusion of substantial distinction in users’ awareness between “professional user-creators” (who get paid for uploading content) and “amateur user-creators” (who upload content merely for social interaction purposes) in most cases. Our findings do support some distinction, however. See *infra* Section III.C.2.c).

156. Cf. Dowthwaite et al., *supra* note 71. (focusing only on “professional” user-creators not on regular users); Fiesler et al., *supra* note 97 (ignoring this distinction altogether).

157. We are aware of another study that similarly investigated ToS of general UGC websites (e.g., IMDA, Craigslist, Y-Gallery); this study, however, had a only few social media platforms in their dataset and a significantly smaller sample overall (410 users). See Fiesler et al., *supra* note 97.

answer.¹⁵⁸ Using Reddit as an example, Figure 2's right two columns present the awareness inquiry as it appeared to the respondents.

The statements presented to the respondents correspond to six of the seven key elements that we identified in Section III.B: perpetuity, third parties (transferability), modification, derivative works, immediate removal, and commercial usage.¹⁵⁹ We did not ask about "other" elements (moral rights, publication rights, and ideas) because, as of the survey date, the majority of our dataset's platforms did not address these elements.¹⁶⁰ Figure 2's left column, which was not part of the survey, classifies the survey's inquiry statements concerning our Section III.B elements.

158. *See infra* Appendix B (Survey Section 6, question 2).

159. *See supra* Section III.B.1.

160. *See supra* Section III.B.2 (Figure 1). We did address the issue of attribution, which is considered a moral right, under the expectation segment of our survey. *See supra* Section III.C.1.c).

Figure 2: Sample Platform Awareness Inquiry (for Reddit)

| <i>Elements</i> | <i>For Reddit, mark one option for each statement— According to its terms:</i> | <i>Yes</i> | <i>No</i> | <i>I don't know</i> |
|--------------------------|--|-----------------------|-----------------------|-------------------------|
| <i>Third parties</i> | Reddit may grant others (third parties) license to use my work | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <i>Modification</i> | Reddit may modify my work | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <i>Derivative works</i> | Reddit may create new works based on my work | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <i>Immediate removal</i> | Reddit may remove content upon their sole discretion | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <i>Commercial</i> | Reddit may use my work for any commercial purpose | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | Reddit may place advertisements on my work | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | Reddit may use my work to promote the platform services | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <i>Perpetuity</i> | Reddit may display my work indefinitely, even if I delete my account | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | Reddit may display my work until I delete my account | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Other than establishing the lack of terms' readability, previous studies (mostly in the privacy sphere) also suggested that, even if users read boilerplate terms, many would find them too difficult to comprehend.¹⁶¹ Our analysis of UGC licensing terms similarly indicate that users require a postgraduate level of reading comprehension to understand those terms.¹⁶² To further examine whether and to what extent users struggle to understand legal terminology, we asked respondents two general questions about the meaning of specific contractual terms (these questions were identical for all survey respondents irrespective of the platforms they indicated using).

In one question, we asked respondents what platforms mean when they ask users in their ToS to “waive [their] so-called moral rights?”¹⁶³ This phrase, taken from Vimeo's ToS, served as a colorful illustration for an instance in which platforms incorporated complex legal terminology with no proper

161. See *supra* note 118.

162. See *Supra* notes 117–119 and accompanying text.

163. See *infra* Appendix B (Survey Section 8, question 1).

clarification.¹⁶⁴ Respondents were then presented with five alternative answers and asked to mark “all that apply.” Two answers were incorrect: “I will not be paid any royalties,” and “I waive all the copyrights in my work.” Two other answers were correct: “It can present my work without my name” (referring to the right of attribution), and “it can change the meaning of my work and distort it in a manner which is disrespectful” (referring to the right of integrity).¹⁶⁵ The final answer—“I don’t know what ‘moral rights’ are”—was neutral.

In a different question, we asked respondents what it meant to grant platforms “a license to prepare derivative work[s]?”¹⁶⁶ We asked about the term “derivative works” because this term is somewhat legally complex (although less so compared to the term “moral rights”) but was nevertheless present in the ToS of most platforms in our dataset.¹⁶⁷ For this question, respondents could again choose among five alternative answers, but we asked them to mark only one answer as correct: (1) “I grant a perpetual (permanent) license to all the rights I have in my work”; (2) “I allow the platform to copy and share my work”; (3) “I allow the platform to place advertisements on my work without my consent”; (4) “I allow the platform to create new versions of my work”; and (5) “None of the above.”

c) Expectations

The purpose of the expectations portion of our survey was to map the respondents’ general intuition and beliefs regarding the scope of an ideal UGC licensing policy. Accordingly, unlike the awareness segment, which only asked respondents about their content-uploading habits for specific platforms, here we asked respondents about their expectations more broadly and not in a way tailored to any specific platform. We asked the respondents five questions about their expectations. Figure 3’s right two columns show these questions

164. Cf. Elizabeth Townsend Gard & Bri Whetstone, *Copyright and Social Media: A Preliminary Case Study of Pinterest*, 31 MISS. C. L. REV. 249, 275 (2012) (suggesting that platforms have a moral responsibility to educate users about their rights). Although U.S. social media users do not enjoy moral rights protection in their UGC, see *supra* note 7, studies have hinted that user-creators deeply care about these rights (especially attribution). See Dowthwaite et al., *supra* note 71 (noting that artists get particularly upset about removal of attribution); cf. Creative Commons Licenses, CREATIVE COMMONS, <https://creativecommons.org/use-remix/cc-licenses/> (last visited Feb. 26, 2020) (fixing attribution as a fundamental right that exist in all types of Creative Commons copyright licenses). Our study also provides overwhelming support for the proposition that user-creators care about attribution. See *supra* Section III.C.2.e).

165. See *supra* note 112.

166. See *infra* Appendix B (Survey Section 8, question 2).

167. See *supra* Section III.B.2 (Figure 1).

and possible answers. Four of the five questions correspond to four of the seven key elements that we identified in Section III.B. One question, however, was about the breadth of platforms' permissible use of UGC and did not fit squarely with any of our stated elements. The element classification appearing on Figure 3's left column was not part of the survey.

Figure 3: Expectations Inquiry

| <u>Elements</u> | <u>Questions</u> | <u>Possible Answers</u> |
|-------------------------------------|--|---|
| <i>Perpetuity</i> | In your opinion, display and distribution of your work should be available [mark one option]: | <ul style="list-style-type: none"> <input type="radio"/> Only for as long as I maintain an account on the platform. <input type="radio"/> Only for as long as I agree. <input type="radio"/> Only until I chose to remove my work. <input type="radio"/> Indefinitely. |
| <i>Immediate removal</i> | In your opinion, sharing platforms should be allowed to [mark the most appropriate option]: | <ul style="list-style-type: none"> <input type="radio"/> Remove content they determine, upon their sole discretion, that violates their terms. <input type="radio"/> Remove content for any reason. <input type="radio"/> Remove content only they are required to do so under law. <input type="radio"/> None of the above. |
| <i>Commercial</i> | In your opinion, social media platforms should be able to [mark all that apply]: | <ul style="list-style-type: none"> <input type="radio"/> Use, display, or distribute my work only for the purpose of the platform's function (social communication). <input type="radio"/> Use, display, or distribute my work for the purpose to promote the platform or the platform's service. <input type="radio"/> Use, display, or distribute my work for any purpose, including for commercial use. <input type="radio"/> Use, display, or distribute my work for the purpose of training artificial intelligence algorithms (machine learning). <input type="radio"/> None of the above. |
| <i>Third parties</i> | In your opinion, who should be allowed to display and distribute your work? [mark all relevant options]: | <ul style="list-style-type: none"> <input type="radio"/> The platform. <input type="radio"/> Its users. <input type="radio"/> Other parties, at the discretion of the platform. <input type="radio"/> No-one. |
| <i>* Breadth of permissible use</i> | In your opinion, a platform should be able to [mark one option]: | <ul style="list-style-type: none"> <input type="radio"/> Display and distribute my work only on the platform. <input type="radio"/> Display and distribute my work on any means of communication. <input type="radio"/> None of the above. |

d) Saliency

In our survey's final segment, we attempted to evaluate UGC licensing policies' saliency to social media users. As explained, the legal concept of *term saliency*—the degree to which terms are sufficiently prominent to users to impact their decision to use and upload content to social media platforms—is emerging as the primary indicator for evaluating, among other things, the need for regulatory oversight of standard-form contracting markets.¹⁶⁸ Term saliency in the context of UGC policies is also important because previous studies did not consider the issue.¹⁶⁹

To evaluate the saliency of UGC licensing policies to social media users, we presented survey respondents with two tasks. First, we asked them to indicate on a Likert scale (ranging from extremely likely to extremely unlikely) how likely they are to use a platform that practices (or is allowed to practice based on its ToS) each of the seven key elements identified in Section III.B. Figure 4's right column presents the survey's questions (as they appeared to respondents). The left column shows our element classifications (which were not visible to respondents).

168. See *supra* text accompanying note 25 and *infra* note 211.

169. See *supra* note 105.

Figure 4: Terms' Salience Inquiry

| <i>Elements</i> | <i>Consider the following scale <Extremely likely, likely, neither likely nor unlikely, unlikely, extremely unlikely> and indicate how likely you are to use such a platform:</i> |
|--------------------------|---|
| <i>Perpetuity</i> | <ul style="list-style-type: none"> • Its terms say you cannot change your mind and cancel the license (permission) you grant the platform to use/display your work. |
| <i>Third parties</i> | <ul style="list-style-type: none"> • Its terms authorize others (nonusers) to distribute and modify your work. |
| <i>Modification</i> | <ul style="list-style-type: none"> • Its terms, allows to modify your work (for any purpose, not just when technically required). |
| <i>Derivative Works</i> | <ul style="list-style-type: none"> • Its terms allow the creation of new works that are based on your work. |
| <i>Immediate Removal</i> | <ul style="list-style-type: none"> • Your content can be removed for any reason. |
| <i>Commercial</i> | <ul style="list-style-type: none"> • Its terms allow the use of your work for any purpose, including commercial use. • Its terms allow to display ads on your work. • Your work is only used for the purpose of operating its platform and nothing else. |
| <i>Other</i> | <ul style="list-style-type: none"> • Associate your name with your work. • Its terms allow your work to be presented without naming you as the creator. • Your work is used for training AI algorithms (machine learning). |

For the second task, we presented respondents with seven statements corresponding to five of the seven key elements identified in Section III.B and asked them to rank the relative importance of those statements on a 1–7 scale (1 being most important and 7 being the least important). Figure 5's right column presents the survey's questions as they appeared to respondents. The left column shows our element classifications (which were not visible to respondents).

Figure 5: Term Ranking

| <i>Elements</i> | <i>The following statements represent varies [sic] Intellectual Property rights. Please rank them according to their importance to you (1 being the most important and 7 the least important).</i> |
|----------------------|---|
| <i>Perpetuity</i> | <ul style="list-style-type: none"> I am able to change or cancel the license (permission) I give platforms to use my work if I change my mind. |
| <i>Third parties</i> | <ul style="list-style-type: none"> The platform won't be able to authorize other parties (nonusers) to use (display and distribute) my work without my consent. |
| <i>Modification</i> | <ul style="list-style-type: none"> My work won't be significantly modified (unless technically required) without my consent. |
| <i>Commercial</i> | <ul style="list-style-type: none"> My work won't be associated with ads. My work won't be used for commercial purposes without my consent. |
| <i>Other</i> | <ul style="list-style-type: none"> The meaning of my work won't be altered in a manner that is disrespectful without my consent. My work must be displayed/associated with my name. |

Answers to the first question indicated how the respondents thought term awareness would impact their social media uploading behavior.¹⁷⁰ Answers to the second question revealed the relative importance of UGC interests to users, information which helps indicate terms that might become salient to better-informed users.¹⁷¹ After presenting our general salience data, we examine whether a significant difference in findings exists between respondents of different usage values.¹⁷²

2. Findings

a) Demographics

Our survey consisted of 1,100 respondents (N=1,100): 51.55% male, 47.91% female, and 0.55% identified as other (rounded). Figure 6 shows the age distribution, with the majority of respondents aged 25 to 34 (43.64%). Figure 6 also shows respondents' income distribution with 30.91% of respondents reporting an income of 25,000 to 50,000 USD and 24.36% reporting an income of 50,000 to 75,000 USD.

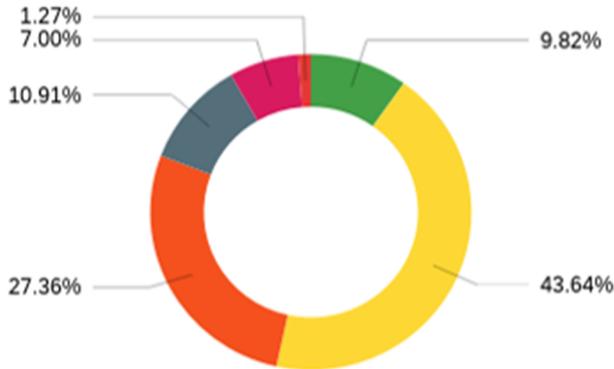
170. Of course, this is merely a partial indication. To fully apprise salience additional work is needed. *See infra* note 203 and accompanying text.

171. Under the notion of salience, the more important an interest or right to a set of user-creators, the more likely it is that a substantial number of them would actually change their social media "sharing" behavior upon receiving more information about how a term affects their interest or right, but *only if* this information is readily understandable. *See* Perzanowski & Hoofnagle, *supra* note 87, at 321–22.

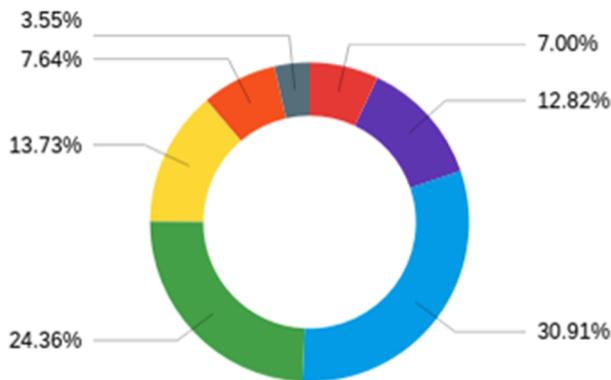
172. *See infra* Section III.C.2.e) (Figure 16).

Finally, Figure 6 shows the respondents' educational background distribution. As indicated, most respondents hold a bachelor's degree. We screened 67 (6.09%) of our respondents after reporting that they did not upload any content to the applicable platforms. That left us with 1,033 respondents.

Figure 6: Demographics Sample



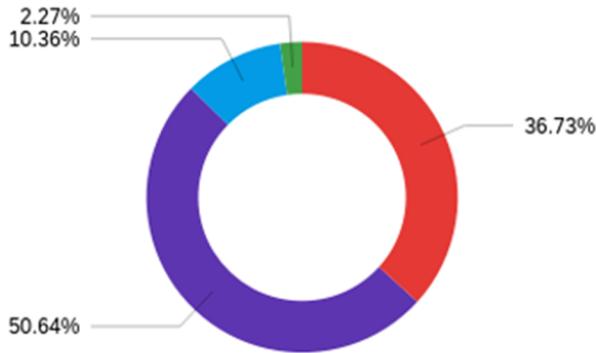
Age Distribution



Income Distribution



Figure 6: Demographics Sample (continued)



Educational background

- High school graduate - high school diploma or the equivalent (for example: GED)
- Bachelor's degree (for example: BA, AB, BS) ■ Master's degree
- Professional degree or doctorate degree (for example: MD, DDS, DVM, LLB, JD, PhD, EdD)

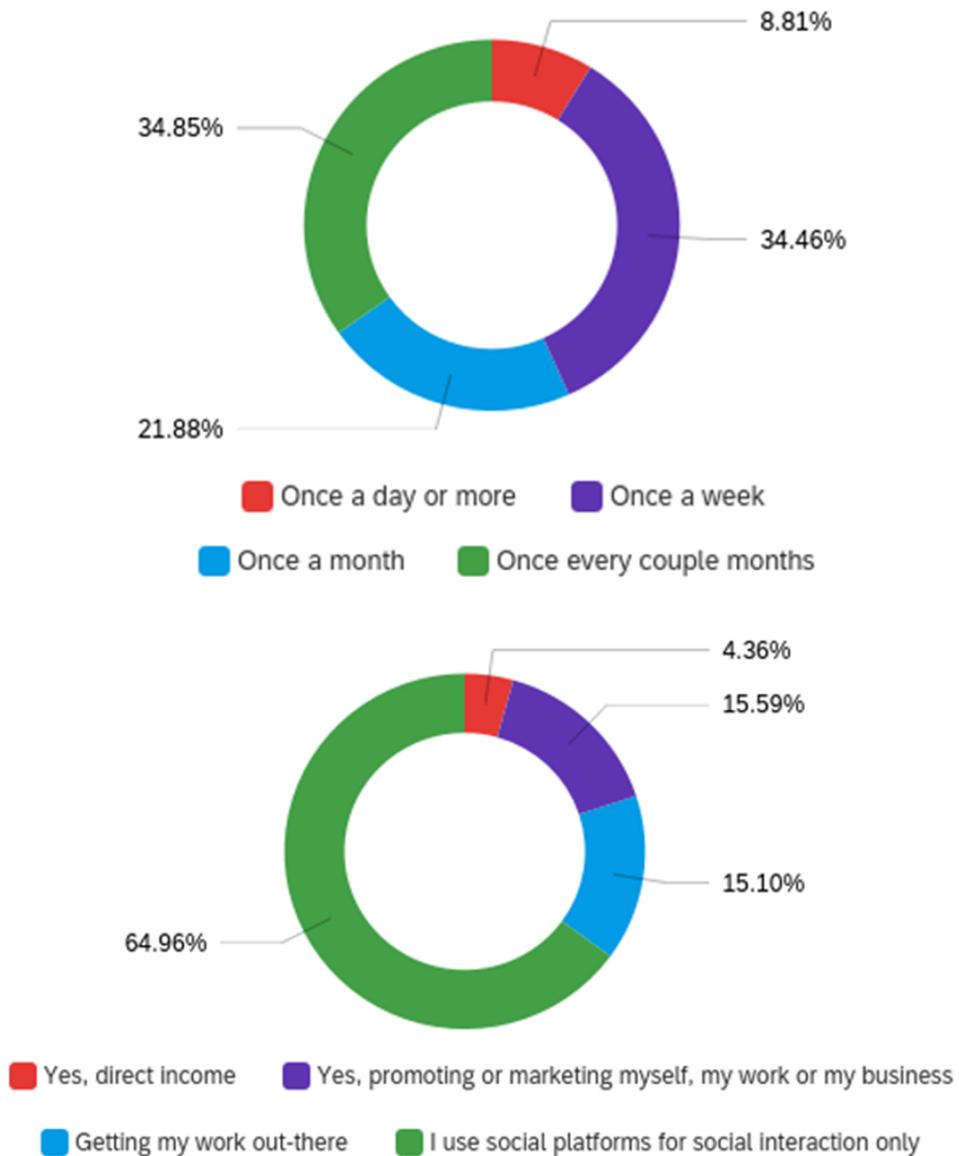
b) Social Media Usage

Survey respondents were asked about how frequently they upload content to social media platforms and about the value they obtain from doing so. From the screened respondents' pool (N=1,033), the majority (64.96%) reported using social media platforms for "social interaction only." 15.10% reported uploading content to platforms for "getting their work out there," 15.59% reported uploading content to promote themselves or their business, and merely 4.36% reported receiving direct income from uploading content (we refer to this small group as "professional user-creators" to distinguish them from "amateur user-creators").¹⁷³

Next, we asked how often users upload their content to social media platforms. Figure 7 shows our findings that 34.8% of respondents upload content once every couple of months, 34.4% upload content once a week, 21.88% once a month, and only 8.81% upload daily or more.

173. See *infra* note 194.

Figure 7: Social Media Usage (Frequency and Value)

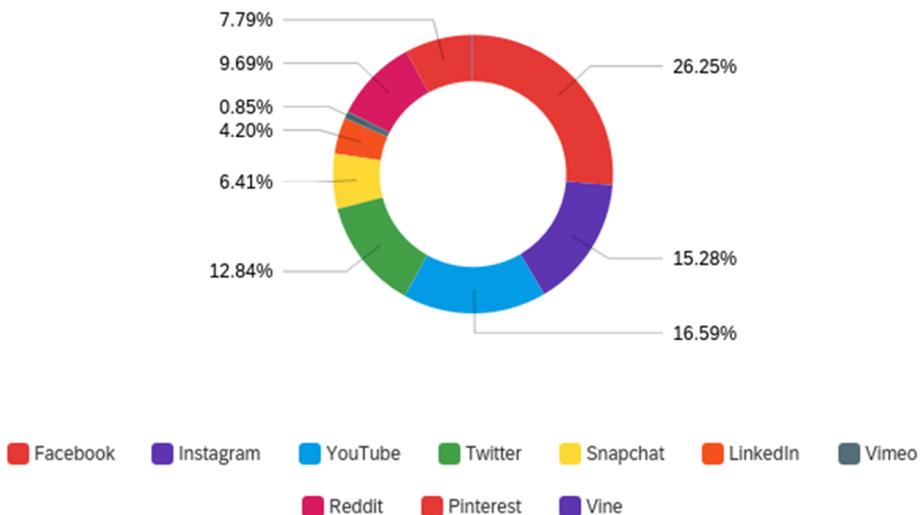


Finally, we asked respondents to which platforms in our dataset they upload their UGC (and respondents could pick multiple platforms, if applicable).¹⁷⁴ Of the content-uploading respondents seen in Figure 8 (N=1,033), 26.25% (rounded) reported uploading to Facebook, 16.59% reported uploading to YouTube, 15.28% reported uploading to Instagram,

174. See *infra* Appendix B (Survey Section 6, question 1).

12.84% reported uploading to Twitter, 9.69% reported uploading to Reddit, 7.79% reported uploading to Pinterest, 6.41% reported uploading to Snapchat, 4.20% reported uploading to LinkedIn, 15.28% reported uploading to Vine, and only 0.85% (26 respondents) reported uploading to Vimeo. This information helped tailor the questions regarding term awareness to the respondents' usage habits.

Figure 8: Social Media Usage (Platform Distribution) (N=1,033)



c) Awareness and Understanding

Respondents were asked to demonstrate term awareness only for the specific platforms to which they indicated uploading content. Figure 9, for example, shows how the survey posed statements about Reddit's terms to users. The table's middle column presents the statements as seen by the Reddit respondents. The left column presents statements' classification based on the key elements identified in Section III.B (this portion was not visible to users). And the right column presents the distribution of the respondents' answers (a complete distribution of term awareness findings per platform appears in Appendix C).

Figure 9: Platform Awareness Inquiry (for Reddit)

| <i>Elements</i> | <i>For Reddit, mark one option for each statement—According to its terms:</i> | <i>Yes</i> | <i>No</i> | <i>I don't know</i> |
|--------------------------|---|------------|-----------|---------------------|
| <i>Third parties</i> | Reddit may grant others (third parties) license to use my work. | 18.0% | 46.8% | 35.3% |
| <i>Modification</i> | Reddit may modify my work. | 24.8% | 46.8% | 27.8% |
| <i>Derivative works</i> | Reddit may create new works based on my work. | 24.1% | 39.7% | 36.3% |
| <i>Immediate removal</i> | Reddit may remove content upon their sole discretion. | 81.7% | 7.5% | 10.9% |
| <i>Commercial</i> | Reddit may use my work for any commercial purpose. | 27.8% | 37.3% | 34.9% |
| | Reddit may place advertisements on my work. | 48.5% | 25.8% | 25.8% |
| | Reddit may use my work to promote the platform's services. | 39.0% | 25.8% | 35.3% |
| <i>Perpetuity</i> | Reddit may display my work indefinitely, even if I delete my account. | 46.8% | 28.8% | 24.4% |
| | Reddit may display my work until I delete my account. | 53.9% | 20.0% | 26.1% |

Our findings shown in Figure 9 suggest that most social media users are grossly unaware of the legal terms governing their UGC. For example, only 18% of respondents knew that Reddit could grant third parties a license to use their work, only 24.8% were aware that Reddit could modify their work or create new works based on their work, and only 27.8% knew that Reddit could commercialize their work for any purpose.¹⁷⁵

Figure 10 provides a wider overview by presenting the average term awareness of all respondents across our entire dataset. The picture portrayed by this figure is similar to the one presented by the Reddit sample in Figure 9. For example, only 20% of all respondents indicated they think social media

175. According to its ToS, Reddit can do all these things. However, Reddit has omitted the provision providing it an all-inclusive commercial-use license. Reddit, *User Agreement*, *supra* note 4.

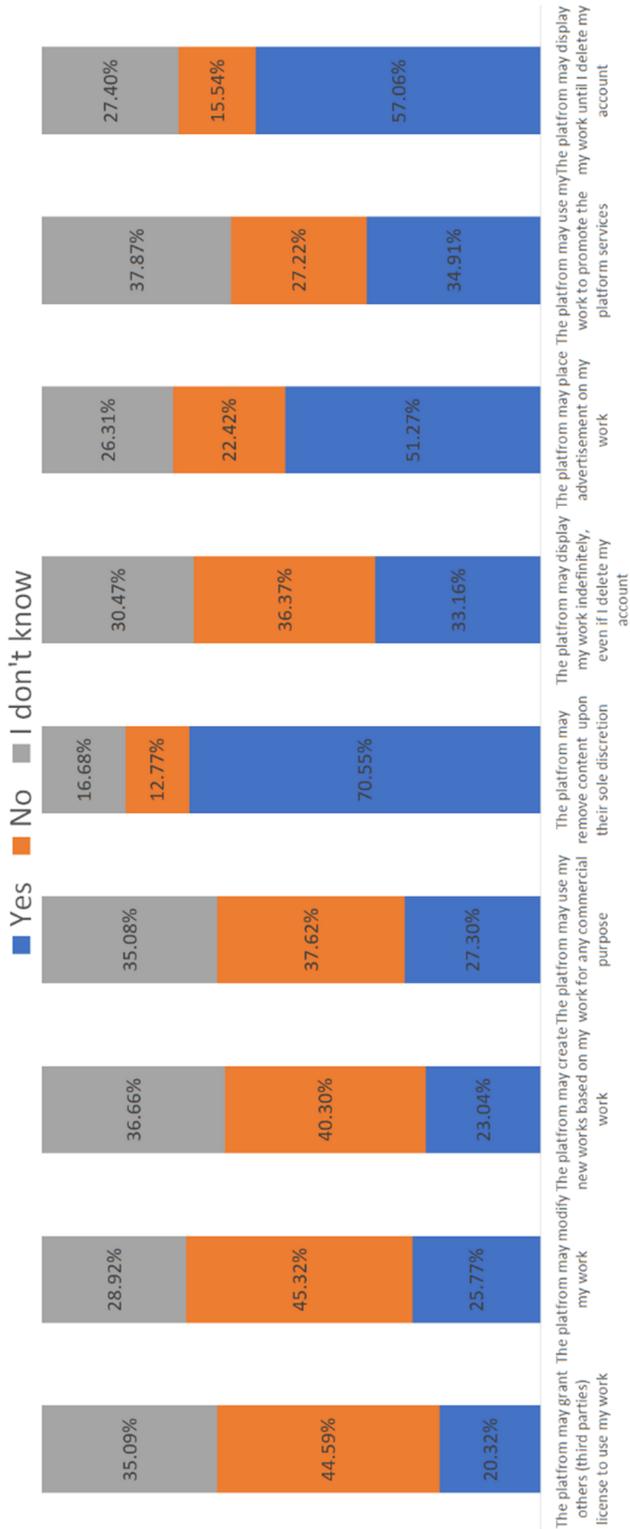
platforms can grant third parties a license to use their work, but the ToS of all platforms in our dataset at the time of the survey enabled platforms to do that.¹⁷⁶ Similarly, 26% and 23% of respondents believed that social media platforms could not modify their work or create derivative works, respectively, but the ToS of most surveyed platforms allowed them to do both.¹⁷⁷ Overall, our findings indicate that users are unlikely to read the ToS that govern their content. This aligns with the conventional wisdom that users rarely read ToS or digital contracts in general.¹⁷⁸

176. *See supra* Section III.B.2 (Figure 1).

177. Of all the surveyed platforms, four platforms (YouTube, Instagram, Reddit, and Vimeo) did not state they can modify their users' work, and four (Instagram, Twitter, LinkedIn, and Vine) did not state they can create derivative works. *See id.*

178. *See supra* notes 87–91 and accompanying text.

Figure 10: Summary of Term Awareness Across Platforms (on Average)



The hypothesis that most users do not read the ToS is supported by data indicating which terms most users either did or did not know existed. These terms unsurprisingly correlated with the platform behavior most users experience in their daily engagement with the platform's service. Of the respondents, for example, 57% knew that social media platforms could display their content at least as long as they retain an active account (something evident merely from seeing photos on Instagram).¹⁷⁹ Similarly, 71% of respondents knew that platforms could unilaterally remove their content (something that many users experience, such as when YouTube videos are taken down for an alleged copyright violation).¹⁸⁰

Moving from awareness to understanding, Figure 11 shows a significant percentage of the survey respondents struggled to comprehend the meaning of “moral rights,” and some respondents even found the term “derivative works” challenging. For moral rights, most respondents' answers (56%) were either wrong or indicated that the respondents “don't know what ‘moral rights’ are.”¹⁸¹ Similarly, many respondents (32%) opted for incorrect answers when asked about derivative works, despite the question being multiple choice and worded so that even uninformed respondents could gather its meaning via context.¹⁸² These findings confirmed our initial concern that social media users

179. As expected, fewer respondents (33%) knew that their content could be presentable even after they deleted their social media account. Still, this number is surprisingly high, which suggests that users are growing to realize that once content is “shared” on social media, it is very difficult to “unshare.” See *supra* note 12.

180. Under the DMCA notice and take down regime, content sharing platforms are required to remove copyright-infringing content upon the copyright owner's notice. 17 U.S.C. § 512 (c)(1)(A)(1998). At the same time, however, technical solutions deployed by platforms—such as YouTube's Content ID system, which allow certain copyright owners to identify potential violations of copyright-protected content uploaded to YouTube—support automatic removal of content. Such automatic removal mechanisms may raise policy concerns—for example, how to treat content that is fair use. This issue was discussed at length in *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150, 1155 (N.D. Cal. 2008). In one of the later proceedings, the Ninth Circuit adopted a broad conception of fair use, explaining that “[f]air use is not just excused by the law, it is wholly authorized by the law.” *Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1151 (9th Cir. 2015). For a general discussion of the DMCA and the takedown regime, see 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, highlight the importance of substantive copyright in the context of online expression); see also Katrina Geddes, *Meet Your New overlords: How Digital Platforms Develop and Sustain Technofeudalism*, 43 COLUM. J. L. & ARTS 455, 462 (2020); Elazari Bar On, *supra* note 25, at 613.

181. See *infra* Appendix B (Survey Section 8, question 1).

182. See *infra* Appendix B (Survey Section 8, question 2).

face legalese that many of them cannot and should not reasonably be expected to understand.

To sum up, in line with related studies on privacy, our findings confirm that social media users are unlikely to read and are struggling to understand the UGC licensing terms of the platforms' service agreements. As such, these policies are *nonsalient*; because users do not have awareness of the terms, they cannot affect users' market decision-making.¹⁸³ We explore the implication of a lack of UGC term salience in Part IV.

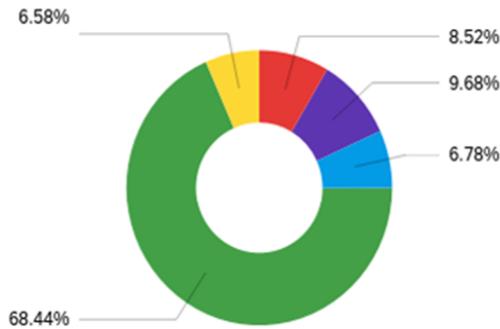
183. Note, however, that users might be aware of a term, but it still would not affect their market decision-making (it would be nonsalient) due to other reasons—for instance, if no alternative terms are being offered in the market (“monopolistic” terms’ market). For further discussion *see supra* note 25.

Figure 11: Term Understanding (“Moral Rights” and “Derivative works”)



When a platform mentions in its terms that “you waive your so-called moral rights” it means:

- I am not paid any royalties
- It can present my work without name
- I waive all the copyrights in my work
- It can change the meaning of my work and distort it in a manner which is disrespectful
- I don't know what "moral rights" are



When a platform mentions in its terms that “you grant the platform a license to prepare derivative work” it means that:

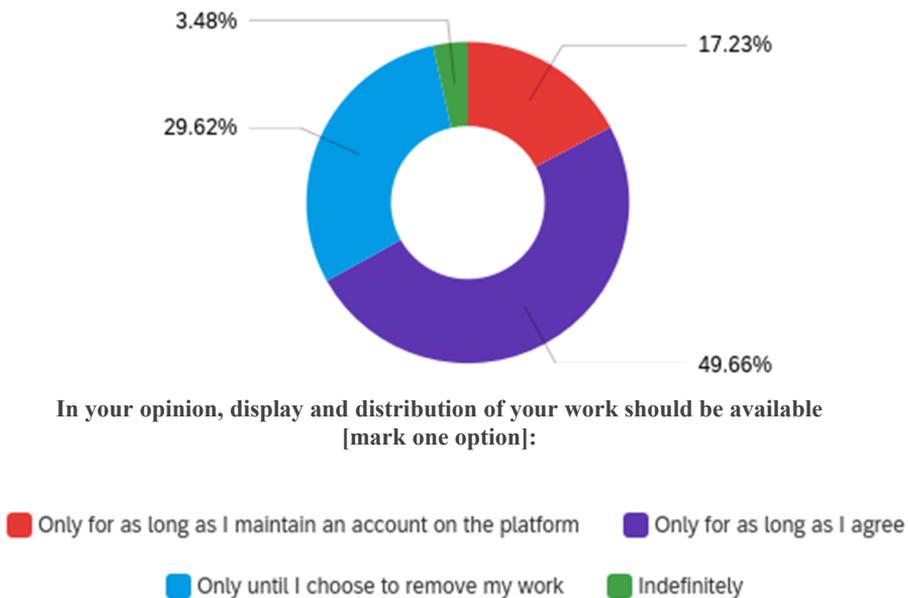
- I grant a perpetual (permanent) license to all the rights I have in my work.
- I allow the platform to copy and share my work.
- I allow the platform to place advertisement on my work without my consent.
- I allow the platform to create new versions of my work.
- None of the above

d) Expectations

Irrespective of the platforms' ToS or users' rights under current copyright law, our survey's expectations segment allowed respondents to indicate their preferences about the ideal scope of a UGC license. These questions revealed what social media users view as the most important elements from *their* perspective. Interestingly, our findings indicate little correlation between respondents' expectations and legal reality.

For example, Figure 12 shows that 50% of recipients indicated that, in their opinion, their work should be available only for as long as they "agree" and merely 3% specified that their work should be available indefinitely. The terms of nearly all the platforms in our dataset, however, specifically provide perpetual UGC licenses that would technically allow platforms to display and distribute users' content indefinitely.¹⁸⁴

Figure 12: Users' Perceptions (Perpetuity)

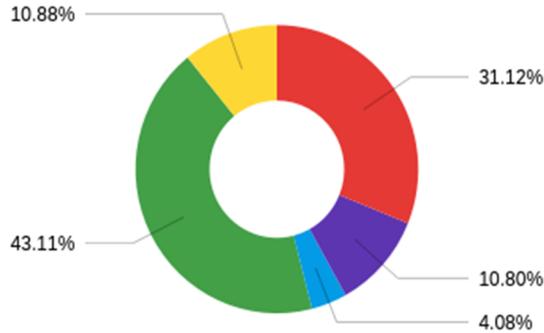


As similarly indicated in Figure 13, among the survey recipients who accepted that social media platforms should be allowed to display and distribute user content at all, the greatest pool of respondents (31%) sought to limit usage to only the platform's functional purpose (social communication).

184. Of all the surveyed platforms, two platforms (Instagram and LinkedIn) did not state they can license their users' work perpetually. *See supra* Section III.B.2 (Figure 1).

Conversely, only 4% of respondents wished to grant platforms the discretion to display and distribute their content for commercial purposes, something that nearly all the platforms in our dataset specifically require.¹⁸⁵

Figure 13: Users' Perceptions (Commercial)



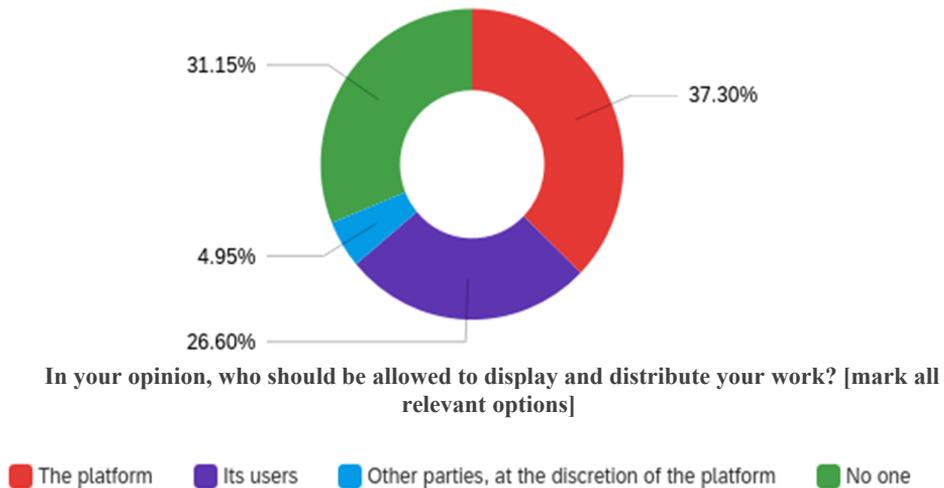
- Use, display or distribute my work only for the purpose of the platform's function (social communication)
- Use, display or distribute my work for the purpose to promote the platform's or the platform service
- Use, display or distribute my work for any purpose, including commercial use
- None of the above
- Use, display or distribute my work for the purpose of training artificial intelligence algorithms (machine learning)

Finally, as seen in Figure 14, only 5% of the survey's recipients indicated that third parties (chosen by the platforms) should be allowed to display or distribute their work, something that *all* the platforms in our dataset require.¹⁸⁶

185. See *supra* Section III.B.2 (Figure 1).

186. See *supra* Section III.B.2 (Figure 1).

Figure 14: Users' Perceptions (Third Parties)



Overall, our findings in this Section paint a striking difference between respondents' expectations and reality. Platforms could not fully adhere to respondents' expectations without completely altering their business models.¹⁸⁷ Still, platforms could very easily make some minor adjustments to UGC licensing policies to better meet respondents' expectations without undermining their services. For example, platforms could disclaim the right to affirmatively display or distribute users' content once users terminate their account.¹⁸⁸ Platforms could also tailor the permissible commercial-use activity to only include promoting their service (as opposed to any imaginable

187. Most social media platforms are advertising companies; they must be able to show ads on their service to maintain this business model. *See supra* note 134.

188. LinkedIn, for example, did just that. Under its current terms, LinkedIn promises that the UGC will not appear on the platform after users have terminated their account unless: (1) for a short period that is technically necessary, or (2) other users have saved and reshared the content. *See infra* Appendix A. Most other platforms, however, do not specifically make such a disclaimer. Instagram ToS, for example, provide that even after users terminate their account, their "[m]aterials and data may persist and appear within the Service." Instagram mentions the scenario in which "[c]ontent has been reshared by others," as an example for why UGC might persist on their service perpetually, but they do not specifically disclaim other scenarios. *See infra* Appendix A.

commercial use).¹⁸⁹ As discussed in Part IV, some of these minor adjustments are already underway.¹⁹⁰

e) Salience

As explained, salience is the degree to which term awareness manifests in real market behaviors.¹⁹¹ In our context, UGC policies would be salient to users if, when presented the terms and understanding the terms' meanings, users would tailor their social media uploading behavior accordingly. To shed light on the question of salience, we charged respondents with two tasks. First, we asked respondents (most of whom were unaware of the platforms' terms¹⁹²) whether and to what extent they would be willing to upload their content to platforms that include various content licensing conditions under their ToS.

Our findings (summarized in Figure 15) indicate that most social media users claim they would significantly change their upload behavior if they knew more about platforms' UGC licensing policies.¹⁹³ For example, the vast majority of respondents (79%) indicated they are unlikely (35%) or extremely unlikely (44%) to use a platform with terms that authorize third parties to distribute or modify their work—something that all the platforms in our dataset currently require. Similarly, most survey respondents (79%) indicated they are unlikely (36%) or extremely unlikely (43%) to use a platform that is allowed to modify their work—something that most platforms in our dataset currently require. Similar inclinations also appeared with respect to platforms' ability to present content without attribution (43% said they are unlikely or extremely unlikely to use), to use and display content after users revoke their authorization (74% said they are unlikely or extremely unlikely to use), and to create derivative works (67% said they are unlikely or extremely unlikely to use).

189. Most platforms do include some limitation on their right to commercialize UGC. Reddit, at the time of the study, had the broadest licenses to commercialize UGC, but it too has since eliminated this broad language. *See* Reddit, *supra* note 4; *infra* note 283.

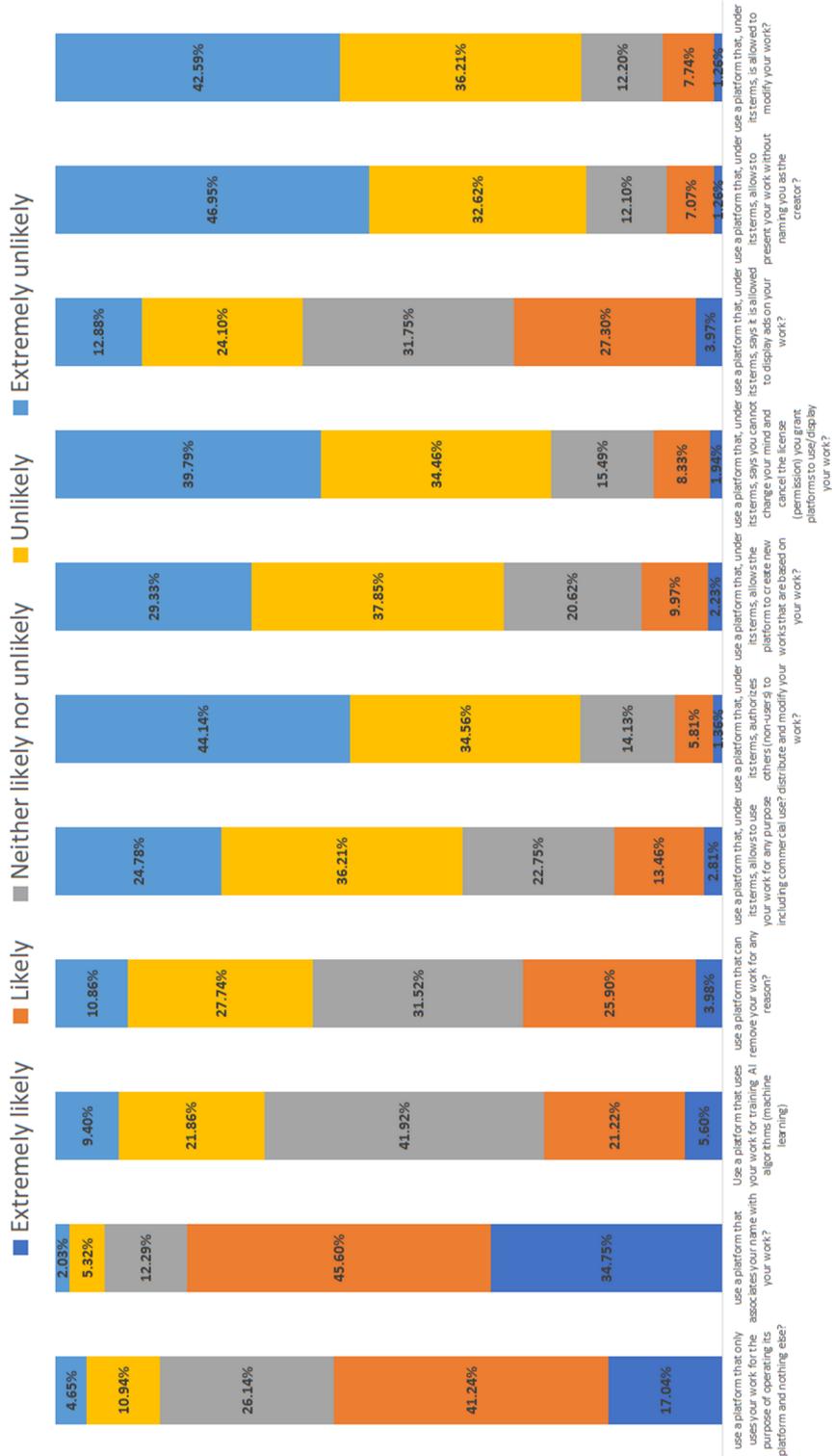
190. *Id.*; *see also* notes 234–238 and accompanying text.

191. *See supra* note 25.

192. *See supra* Section III.C.2.c).

193. These findings should be taken with a grain of salt, however. To fully apprise salience, future work is needed. *See infra* note 203 and accompanying text.

Figure 15: Terms' Saliency Inquiry



While these overwhelming trends do not change significantly after filtering our findings and classifying them based on users' usage habits, minor changes appear at the margins. For example, "professional user-creators" (those who receive direct financial value from uploading content) were far less zealous than "amateur user-creators" (those who upload content solely for social interaction purposes) with respect to at least some of the investigated elements.¹⁹⁴ Figure 16, for example, indicates that more professional users were "likely" and "extremely likely" to use platforms that commercialize their content (36%) or that do not enforce attribution (18%) compared to amateur users (15% and 7%, respectively). These findings do not necessarily mean professional user-creators care less about commercialization or attribution than amateur user-creators; they merely suggest that the former are willing to trade such rights for financial compensation.

194. *See infra* Section III.C.2.c).

Figure 16: Term Salienc Inquiry (Professional vs. Amateurs)

How likely you are to use a platform that under its terms allow [sic] to use your work for any purpose, including commercial? purpose?

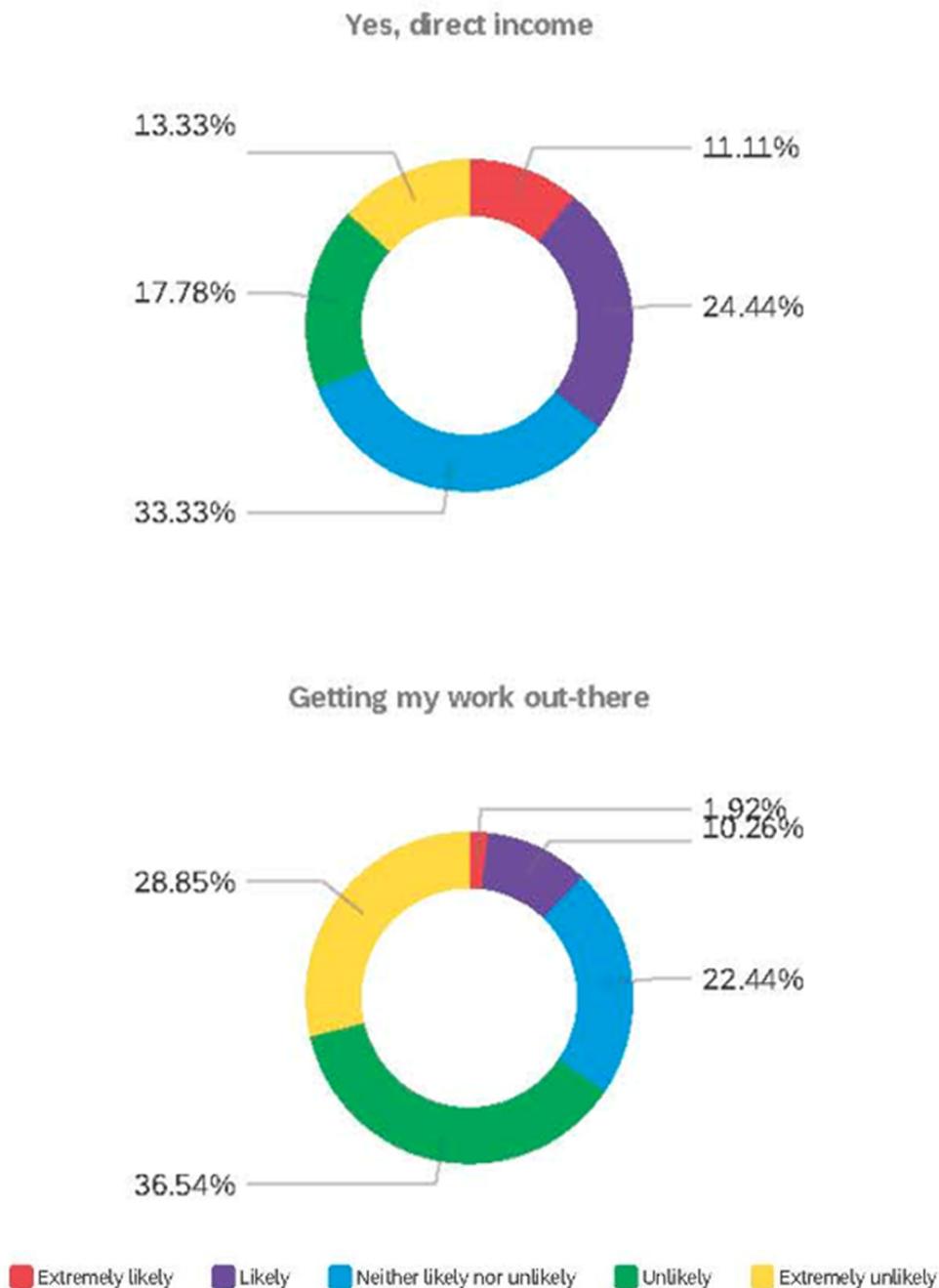


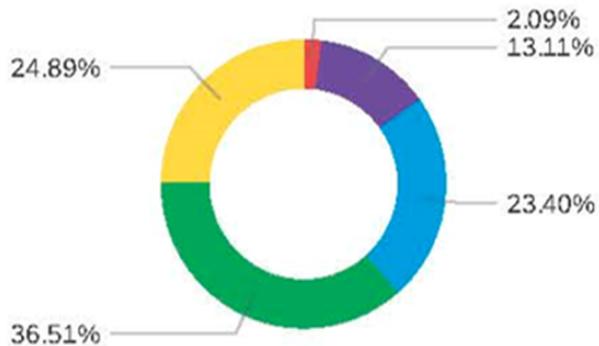
Figure 16: Term Salience Inquiry (Professional vs. Amateurs) (continued)

How likely you are to use a platform that under its terms allow [sic] to use your work for any purpose, including commercial? purpose?

Yes, promoting or marketing myself, my work or my business



I use social platforms for social interaction only



■ Extremely likely
 ■ Likely
 ■ Neither likely nor unlikely
 ■ Unlikely
 ■ Extremely unlikely

Figure 16: Term Salience Inquiry (Professional vs. Amateurs) (continued)

How likely you are to use a platform that under its terms allow [sic] to present your work without naming you as the creator?

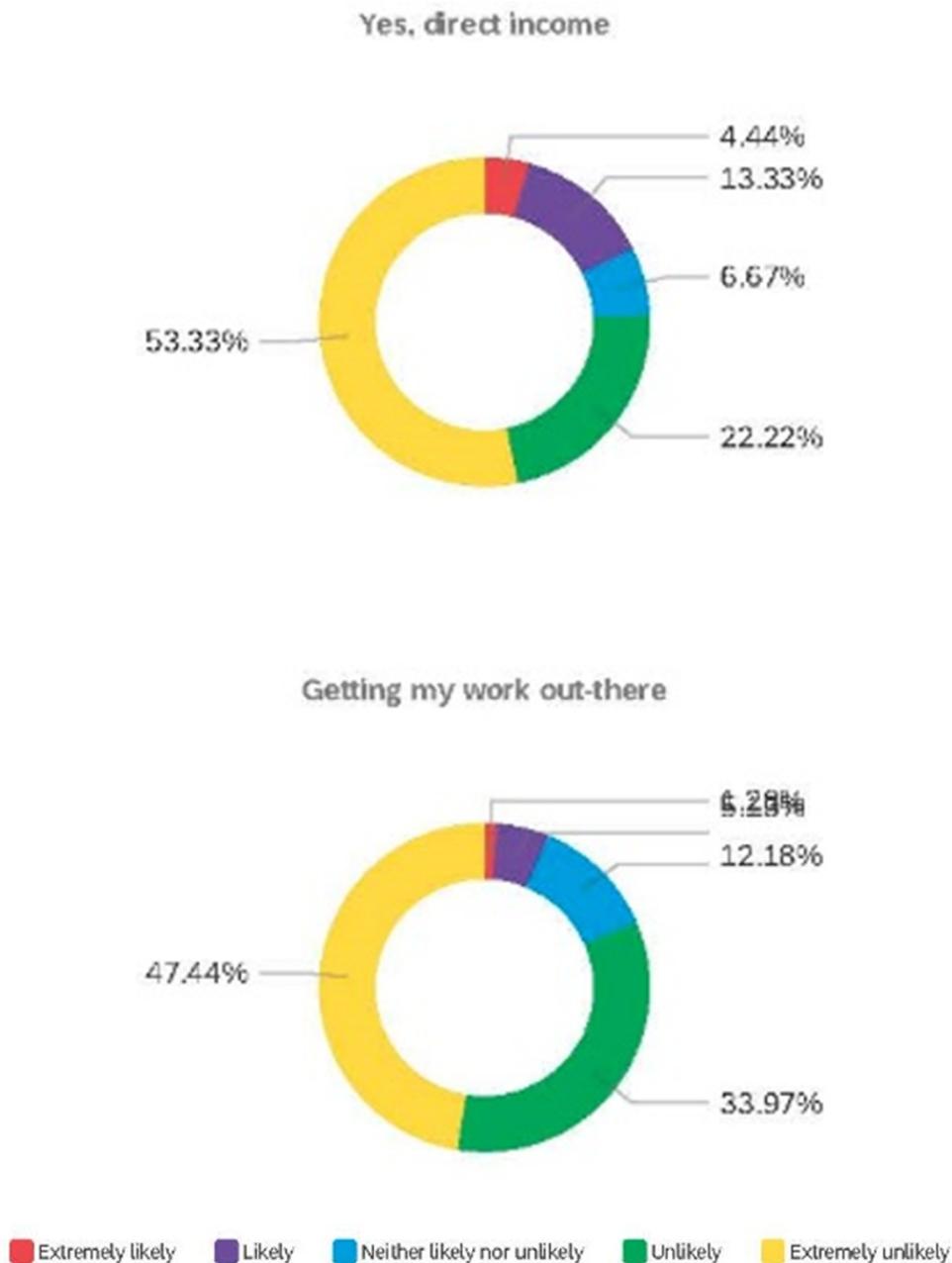


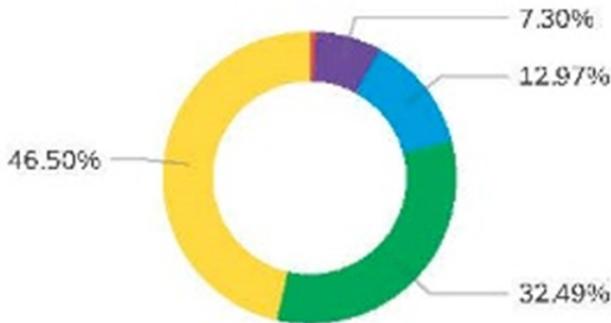
Figure 16: Term Salience Inquiry (Professional vs. Amateurs) (continued)

How likely you are to use a platform that under its terms allow [sic] to present your work without naming you as the creator?

Yes, promoting or marketing myself, my work or my business



I use social platforms for social interaction only



Extremely likely Likely Neither likely nor unlikely Unlikely Extremely unlikely

In the second task designed to shed light on UGC policies' salience to users, respondents ranked seven statements according to importance on a 1–7 scale (1 being most important to them and 7 being least important). This task provides a useful indication of the subjective value users attach to various legal elements relating to their uploaded content. The more value respondents

attach to a specific element, the more likely this element will become salient and drive user uploading behavior.¹⁹⁵

Figure 17 presents each statement's average rank, organized by their relative importance to respondents and classified by element (a full ranking distribution appears in Appendix D).

Figure 17: Term Ranking

| <i>Element</i> | <i>Statement</i> | <i>Average Ranking</i> |
|----------------------------|--|------------------------|
| <i>Other (attribution)</i> | My work must be displayed/associated with my name. | 2.82 |
| <i>Perpetuity</i> | I am able to change or cancel the license (permission) I give platforms to use my work if I change my mind. | 3.53 |
| <i>Commercial</i> | My work won't be used for commercial purposes without my consent. | 3.85 |
| <i>Third parties</i> | The platform won't be able to authorize other parties (nonusers) to use (display and distribute) my work without my consent. | 3.87 |
| <i>Other (integrity)</i> | The meaning of my work won't be altered in a manner that is disrespectful without my consent. | 4.04 |
| <i>Modification</i> | My work won't be significantly modified (unless technically required) without my consent. | 4.07 |
| <i>Commercial</i> | My work won't be associated with ads. | 5.81 |

As seen in Figure 17, most respondents ranked attribution as the single most important feature. Notably, none of the platforms in our dataset respect users' right of attribution, possibly because U.S. copyright law does not provide social media users with such a right to begin with.¹⁹⁶ Nevertheless, attribution's heightened importance to user-creators (a fact that is also supported by other sources¹⁹⁷) suggests that policymakers or the platforms themselves should consider helping users enforce this right. We consider this option further in Part IV.

As offered in the preceding Section, platforms could also address perpetuity and commercialization by introducing reasonable limits to their UGC licensing policies.¹⁹⁸ The same can also be said of an unrestricted sublicensing requirement, something most platforms in our dataset require.¹⁹⁹

195. See *supra* note 171.

196. See text accompanying *supra* note 7.

197. See *supra* note 164.

198. See *supra* note 188.

199. See *supra* Section III.B.2. (Figure 1).

Lastly, Figure 17 shows that most respondents consider platforms' ability to associate their content with ads as the least important term. This finding is good for platforms that rely on advertising to generate revenue. Overall, this exercise indicates that, although users acknowledge platforms must maintain their business, they would prefer platforms to better safeguard their UGC interests.

3. *Methodological Limitations*

We acknowledge the limitations of a self-reported survey methodology. The first key issues with a survey instrument are potential non-response biases and the sample not representing the target population.²⁰⁰ To mitigate those concerns and to validate the study's generalization ability, our survey was conducted among a relatively large sample size (~1000) of Mechanical Turk ("MTurk") users. Our design included a single-screening criterion, which only screened out 67 (6.09%) respondents after reporting they did not upload any content to the applicable platforms. No other respondents or populations were excluded. Given the studied topic's nature, we concluded that a web-based survey is most suitable to capture and represent the target population—a U.S. social media adult population.²⁰¹ Executing our survey via MTurk further assured quality control because studies have found that MTurk produces data "at least as reliable as those obtained via traditional methods," establishing a sample likely to be more diverse than those established by other methods.²⁰²

The second pitfall concerns the reliability of self-reported data and possible response biases. Here, we specifically refer to the "value-action gap"—the gap between people's attitudes or perceptions versus actual behavior.²⁰³ This limitation increases when assessing terms' salience.

200. Particularly, a web-based survey might lead to specific biases resulting from underrepresentation of certain groups online. Some studies find lower presence of certain racial or ethnic groups on online platforms, such as African Americans and Hispanic Americans, as well as age discrepancies because older population tends to use technology less. See, e.g., Gabriele Paolacci, Jesse Chandler & Panagiotis G. Ipeirotis, *Running Experiments on Amazon Mechanical Turk*, 5 JUDGMENT & DECISION MAKING 411 (2010). Moreover, there is no current data on what constitutes the global population of UGC-uploading social media users.

201. *Social Media Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), <https://www.pewresearch.org/internet/fact-sheet/social-media/>.

202. See Michael D. Buhrmester, Tracy Kwang & Samuel D. Gosling, *Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data?*, 6 PERSPECTIVES ON PSYCHOLOGICAL SCIENCE 3–5 (2011).

203. For an overview, see Icek Ajzen, Thomas C. Brown, & Franklin Carvajal, *Explaining the Discrepancy Between Intentions and Actions: The case of Hypothetical Bias in Contingent Valuation*, 30(9) PERS. SOC. PSYCHOL. BULL. 1108–21 (2004); see also Icek Ajzen, *Nature and Operation of Attitudes*, 52 ANNU. REV. PSYCHOL. 27–58 (2001). The ultimate way to overcome this difficulty

Acknowledging the advantages of observational studies, the dearth of research in this field, and the cost of collecting behavioral data online, we concluded that a survey is appropriate for collecting data for this study's narrow purposes. Conducting an anonymous survey via a third party (MTurk) allowed us to avoid additional response biases because respondents were given minimal information about the study's aims. We took conventional means to mitigate response biases, such as crafting questions using simple and natural²⁰⁴ language where applicable, randomizing the order of answers, using various answer types, and reversing scales where possible.

IV. POLICY IMPLICATIONS

Commenters disagree about whether and how much courts and legislators should interfere in the free market of contractual obligations and whether to

is by measuring ones' behavior rather than attitude. Thus, as a follow up study, we aim to conduct an experiment geared towards assessing users' behavioral change upon exposure to terms. At the first stage of the experiment, we would solicit participants to upload their original creative content (photographs, videos, poetry, short stories, or articles, and the like) to a designated website as a contest for a prize. Upon uploading their content to the designated competition website, users would have the option to also upload their content to one of several social platforms. Then, users who expressed their desire to share their content on social platforms would see another screen providing them with simplified disclosures of key conditions in the ToS of the specific to platform they chose. This simplified disclosure would be based on the real terms of each platform, relevant at the time of the experiment. For example, these terms might include a commercial-use license to user content, the ability to sub-license the platforms' authority to third parties, etc. Using this interface, we would examine if users *actually* change their behavior after they had been informed of a specific contractual term relating to their copyright in their content at the time they decide to "share" that content. The experiment ends once the user chooses whether or not to upload the content (in any event, content is not shared). We designed the experiment so that content is allegedly uploaded to actual, popular social media platforms. This allows us to avoid the difficulties involved with establishing a new social media network while analyzing real market terms (the actual terms incorporated by the platforms.) This two-phase upload interface is meant to avoid a situation where users are reluctant to share their content for reasons unrelated to the platforms' ToS.

204. Nonetheless, in some instances it would be reasonable to assume that our findings somewhat inflate the level of understanding and knowledge among the sample, compared with actual knowledge among the target population. This is mostly due to the fact that our survey is composed of multiple-choice and scale questions rather than open-ended questions. We believe greater lack of knowledge would have been revealed through open-ended questions. For example, when questioning about the meaning of "derivative work," approximately 70% of respondents knew the correct answer among the five options offered to them. *See supra* Section III.C.2.c). As stated, we believe that had it been an open-ended question, much less than 70% would have provided the correct definition.

outlaw boilerplate terms in form contracts.²⁰⁵ Traditional economic analyses have long established that, in a perfectly functioning market and with complete information, even adhesive contracts between buyers and sellers will always only contain terms that enhance consumers' welfare.²⁰⁶ Professor Russell Korobkin emphasized, however, that buyers are *boundedly rational* rather than fully rational decision-makers (meaning they consider some product attributes and ignore others when making contracting decisions).²⁰⁷ It follows that the laissez-faire approach to boilerplate terms should be bounded as well.²⁰⁸ Specifically, policymakers should trust markets to generate socially desirable terms when buyers consider such terms in their contracting decisions ("salient" terms), but policymakers should be more suspicious of terms that buyers do not consider in their contracting decisions ("nonsalient" terms).²⁰⁹ Regarding the latter, markets will not compel sellers to generate terms that enhance

205. See generally RADIN, *supra* note 78; Slawson, *supra* note 76; Korobkin, *supra* note 25. As a practical matter courts usually view boilerplate terms in digital form contracts as enforceable, at least insofar users have a quality opportunity to read through the agreement. 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."); *Serrano v. Cablevision Sys. Corp.*, 863 F. Supp. 2d 157, 164 (E.D.N.Y. 2012) ("In the context of agreements made over the internet, such "click-wrap" contracts are enforced under New York law as long as the consumer is given a sufficient opportunity to read the end-user license agreement, and assents thereto after being provided with an unambiguous method of accepting or declining the offer."); *Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17, 32–35 (2d Cir. 2002) ("[W]here consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms [R]easonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility.") (footnote omitted). Nevertheless, courts can find specific terms unenforceable, especially if they are uniquely unexpected or "surprising." See, e.g., *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593, 606 (E.D. Pa. 2007) (explaining that burying an arbitration provision in a lengthy paragraph under the heading "GENERAL PROVISIONS" caused surprise to the user and that the term thus satisfied the procedural element of unconscionability).

206. See, e.g., R. Ted Cruz & Jeffrey J. Hinck, *Not My Brother's Keeper: The Inability of an Informed Minority to Correct for Imperfect Information*, 47 HASTINGS L. J. 635, 638 (1996); Eric A. Posner, *Contract Law in the Welfare State: A Defense of the Unconscionability Doctrine, Usury Laws, and Related Limitations on the Freedom to Contract*, 24 J. LEGAL STUD. 283, 284 (1995).

207. See Korobkin, *supra* note 25, at 1204–06.

208. The bounded rationality of buyers is a result of information overload and limitations of attention and cognition. *Id.*

209. Regulation of consumer-salient terms "may be less necessary and may lead to undesirable results, including a reduction in consumer choice." *Id.*

consumers' welfare, and additional regulatory or judiciary oversight might be needed to achieve this goal.²¹⁰

Our findings indicate that users possibly do not read, hardly understand, and have unrealistic expectations regarding UGC licensing policies in platforms' ToS. These findings signal that these policies are nonsalient to users, which may justify some regulatory oversight.²¹¹ We discuss this approach in Section IV.B. On the other hand, our data suggest that social media users care about UGC licensing policies and claim they would change their behavior if

210. In discussing the standards for consumer consent, the Restatement explains that the “concept of salience underlies the metrics regularly used to determine whether a contract term is unconscionable.” THE RESTATEMENT OF THE L. CONSUMER CONT., TENTATIVE DRAFT, at 94–95 (AM. LAW INST. 2019), https://www.ali.org/media/filer_public/05/30/053007a1-2b37-4142-b9c3-7a881e847d50/consumer_contracts_-_td_-_online.pdf. Thus, consumers' consent is vitiated when they face a “lack of meaningful choice” (if a term was nonsalient because it did not “affect consumers' contracting decisions”). *Id.* Consent may also be vitiated where a term constitutes an “unfair surprise,” is “hidden” or “unduly complex,” or results from “uneven bargaining power.” *Id.* These tests “are either synonymous with, or direct results of, nonsalience.” *Id.*; see also Elazari Bar On, *supra* note 25 (discussing the role of salience in the unconscionability doctrines).

211. As explained in *supra* note 25, nonsalient terms are not automatically inefficient, but they can be. A substantive inquiry should also take place to determine whether nonsalient terms are insufficient. Such an inquiry could suggest that nonsalient UGC terms are procedurally unconscionable because the market does not police those terms since they do not affect users' decision-making. Arguably then, due to the non-substitutable value of social media platforms to consumers and parity between UGC terms across platforms, there is no competitive market for UGC terms. Rather, each platform operates as a monopolistic contractor. Nonsalient UGC terms, therefore, may undermine intellectual property policy (to incentivize market competition) and thus are *substantially unconscionable* as well. See Elazari Bar On, *supra* note 25. The unconscionability doctrine includes two components. 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, establishing whether the term actually affects consumers' contracting decisions, and asking whether the market disciplines the term' quality since drafters are incentivized to provide better terms at the risk of losing consumers to the competition. Therefore, it would be harmful and redundant for courts to intervene via the unconscionability doctrine. This second component, substantive unconscionability, pertains to the question of whether the enforcement of the term would be “shocking to the conscience,” and addresses the one-sidedness of a term that unreasonably undermines “the consumer's benefit from the bargain.” *Id.* at 624–26.

On the relation between the nonsalient nature of terms and justification for judicial intervention, see THE RESTATEMENT OF THE L. CONSUMER CONT., TENTATIVE DRAFT, at 94–95 (AM. LAW INST. 2019), https://www.ali.org/media/filer_public/05/30/053007a1-2b37-4142-b9c3-7a881e847d50/consumer_contracts_-_td_-_online.pdf; see also Korobkin, *supra* note 25.

they had better information.²¹² Providing users with better information is relatively straightforward in the UGC licensing arena (unlike in the opaquer privacy arena). Thus, remedial approaches that are less radical than substantive regulation, such as improved disclosures or education campaigns, may sufficiently enhance UGC saliency and allow markets to self-regulate. We discuss this approach in the following section.

A. MARKETS AND SELF-REGULATION

Our data indicate that a substantial portion of social media users care about copyright policies and claim they would change their behavior with better knowledge of UGC policies.²¹³ This suggests that mild market interventions—such as disclosures, education, and changing social norms—might suffice to increase term salience to users and pressure social media platforms to improve their UGC licensing practices. In fact, as was long suggested in law and economics literature, even a small minority of term-conscious social media users could suffice to discipline platforms against using unfavorable boilerplate terms.²¹⁴

Several studies on privacy have documented how changing norms and education increase privacy salience.²¹⁵ One study has shown, for example, that

212. It is also possible that, similar to the “Privacy Paradox,” discussed in *supra* note 34–36 and accompanying text, users may act differently than what they report (the “UGC Paradox”). We recognize this limitation in our work and propose that similar experiments to this conducted in the area of privacy can be conducted in this realm as future work. *See supra* note 203 and accompanying text.

213. *See* Section III.C.2.c.

214. The “informed minority” body of literature explores this argument further. Under this view, a consumer minority who read the terms and conditions is sufficient to create a market force that requires suppliers to adjust themselves to the informed minority’s preferences. In this way, the market will create fair contracts without juridical interference. *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, 645 (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* ELENA D’AGOSTINO, *CONTRACTS OF ADHESION BETWEEN LAW AND ECONOMICS RETHINKING THE UNCONSCIONABILITY DOCTRINE* 62 (2015); Howard Beales et al., *The Efficient Regulation of Consumer Information*, 24 J.L. & ECON. 491, 502 (1981). *But see* Yannis Bakos, Florencia Marotta-Wurgler, and David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 3 (2014) (suggesting, on the basis of empirical analysis, that an informed minority cannot affect the willingness of suppliers to change the contract terms in real market conditions).

215. *See generally* Leslie K. John, Alessandro Acquisti & George Loewenstein, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. CONST. RES. 858, 858–59 (2011) (summarizing the factors that contribute to the “privacy paradox,” focusing on social norms); Korobkin, *supra* note 25, at 1266–68 (pointing to the correlation between better education and increased salience).

users with doctoral degrees possessed the greatest level of privacy concern, successively followed by those with vocational degrees, professional degrees, college education, and high school education.²¹⁶ Other studies confirmed that users with the highest levels of education revealed the fewest optional data elements and that users with a cybersecurity educational background are even more reluctant to reveal their information.²¹⁷ Similarly, studies have shown that changes in social norms over time, across cultures, or among age-groups impact privacy preferences.²¹⁸ Unsurprisingly, following the heightened journalistic coverage and public scrutiny of privacy and cybersecurity issues after the foreign influence and Cambridge Analytics scandals, most platforms decided to reconfigure their privacy policies.²¹⁹

In the same way, academics and public advocates could motivate platforms to improve their UGC licensing policies by securitizing these issues. As Professor Margret Jane Radin recently offered, “NGOs can organize publicity

216. See Dara O’Neil, *Analysis of Internet users’ level of online privacy concerns*, 19(1) SOC. SCIENCE COMPUT. REV. 17–31 (2001).

217. See, e.g., Meredydd Williams & Jason R.C. Nurse, *Optional data disclosure and the online privacy paradox: A UK perspective*, in INTERNATIONAL CONFERENCE ON HUMAN ASPECTS OF INFORMATION SECURITY, PRIVACY AND TRUST AT THE 18TH INTERNATIONAL CONFERENCE ON HUMAN-COMPUTER INTERACTION 193 (2016).

218. Andrea Devenow & Ivo Welch, *Rational Herding in Financial Economics*, 40(3) EUROPEAN ECONOMIC REVIEW 603 (1996) (investigating changes in norms over time); Tawfiq Alashour, Mark Keil, Leigh Liu & Jeff Smith, *How values shape concerns about privacy for self and others*, in INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS (2015) (similar); Elena Daehnhardt, Nick K. Taylor, & Yanguo Jing, *Usage and Consequences of Privacy Settings in Microblogs*, in The 15th INTERNATIONAL CONFERENCE ON COMPUTER AND INFORMATION TECHNOLOGY 667–73 (2015) (reporting on a study of Twitter settings, finding that citizens from Japan were more private than those from Brazil or Spain); Susan B. Barnes, *A privacy Paradox: Social Networking in the United States*, 11(9) FIRST MONDAY (2006) (investigating privacy perceptions across age groups).

219. See, e.g., David Klein & Joshua Wueller, *Fake News: A Legal Perspective*, 20 J. INTERNET L. 1, 10(2017) (“In response to sharp public criticism of the fake news phenomenon, many Internet advertising companies have updated their program policies to deny services to fake news publishers . . .”); Anna Gonzalez & David Schulz, *Helping Truth with Its Boots: Accreditation as an Antidote to Fake News*, 127 YALE L.J. FORUM 315, 318 (2017); Amber Jamieson & Olivia Solon, *Facebook to begin flagging fake news in response to mounting criticism*, THE GUARDIAN (Dec. 15, 2016), <https://www.theguardian.com/technology/2016/dec/15/facebook-flag-fakenews-fact-check.>; Facebook, *How is news marked as disputed on Facebook?*, <https://www.facebook.com/help/733019746855448>; Bernhard Clemm, *Analysis | Facebook wants its users to drive out fake news. Here’s the problem with that*, WASH. POST (Feb. 1, 2018), <https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/01/facebook-wants-to-drive-out-fake-news-by-having-users-rate-news-outlets-credibility-heres-the-problem-with-that/> (last visited June 25, 2018) (reporting on Facebook’s attempt to use a crowdsourcing model for verifying fake news); Elisabeth Dwoskin, *Twitter is looking for ways to let users flag fake news, offensive content*, WASH. POST (June 29, 2017), <https://www.washingtonpost.com/news/the-switch/wp/2017/06/29/twitter-is-looking-for-ways-tolet-users-flag-fake-news/>. See generally Hacoheh & Menell, *supra* note 47.

campaigns to make known to the public what some of the onerous terms in the fine print actually mean. They can take the lead in organizing a rating site that will advise consumers which firms are using reasonable terms and which are not”²²⁰ A task force of lawyers, which the Children’s Commissioner for England convened in 2017, undertook a similarly spirited effort when they tried to simplify Instagram’s ToS to better inform users about their rights.²²¹ This endeavor attracted media coverage, which spurred users’ awareness.²²² Such efforts are becoming increasingly common, especially regarding privacy, cybersecurity,²²³ and false advertising.²²⁴

220. See RADIN, *supra* note 78, at 243.

221. See Wang, *supra* note 97.

222. *Id.* (“[O]nce there is more transparency around how [Instagram’s] site works, we hope that will lead to some consumer pressure from the children and they will start demanding more.”).

223. See The Center for Human Technology, <https://www.humanetech.com/> (last visited Nov. 26, 2020). (a non-profit organization devoted to educating users about the risks of tech manipulation and addiction); see also the NGO “Ranking Digital Rights” (<https://rankingdigitalrights.org/>) (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*). Compare also to the regime in the United Kingdom, where Section 6 of the Unfair Terms in Consumer Contracts Regulations and the Consumer Rights Act 2015 enables certain “regulators” to initiate enforcement action (a complaint) with respect to unconscionable terms. See 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. The United Kingdom’s various regulatory bodies (listed in Schedule 3 to the Act), *id.* at 14, as well as the U.K. Competition & Markets Authority, publish “Guidance” with lists of potentially unfair terms, *e.g.*, *id.*; 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> (“[T]erms which assume consumers have consented to the use of any personal information (including their name) for promotional purposes for the benefit of the operator.”). These regulatory guidelines supplement the “grey list” of presumptively unconscionable terms contained in Schedule 2 of the Consumer Rights Act 2015. 2015 c. 15 (UK).

224. For instance, in the advertising field, see OVERVIEW | MIDDLE SCHOOL CURRICULUM, <https://www.foolproofmiddleschool.com> (last visited Mar. 20, 2018) (“FoolProof” has developed curricula that are used in tens of thousands of schools with the design of teaching children the methods of deception and strategic persuasion. There is some evidence now that, to combat misinformation, teaching the persuasive techniques is more effective than the substance.”); TRUTH IN ADVERTISING, <https://www.truthinadvertising.org> (last visited June 28, 2018) (educating consumers about deceptive advertising practices such as stealth endorsements). In 2018, the digital marketing agency Mediakix created a false social media influencer persona to educate the public on the practices of unjust endorsements on Instagram. Katie Notopoulos, *It’s Easy To Scam Your Way Into Free Hotel Stays By Pretending To Be An Instagram Star*, BUZZFEED (June 25, 2018), <https://>

Furthermore, consumer pressure is likely even more effective in the UGC licensing policies context than in the privacy context. Unlike in the privacy arena, where the opaque nature of privacy harm pushes platforms to stretch their data-monetizing privileges to the fullest, the harms associated with monetizing UGC are far easier for consumers to grasp, which presumably may deter platforms from fully exploiting their overly broad licensing privileges.²²⁵ Thus, unlike in the privacy sphere, platforms have little to lose (and could potentially even benefit) from increased salience, which would invite them to compete for copyright savvy users.²²⁶

In theory, public pressure from educated users might even motivate platforms to provide users with terms that are better than those the law currently provides. This is what happened in the digital advertising sphere following the foreign influence crisis of 2016.²²⁷ Once threats of digital propaganda, fake news, and other forms of voter manipulation intensified, the public's favorable opinion of social media platforms radically shifted.²²⁸ Facing

www.buzzfeed.com/katienotopoulos/its-easy-to-scam-your-way-into-free-hotel-stays-by (last visited June 26, 2018).

225. Users ability to understand the potential risks associated with the terms was referred to in the privacy literature as “risk salience.” See, e.g., Williams, Nurse, & Creese, *supra* note 36 at 3; Bamberger et al., *supra* note 36, at 336.

226. See Korobkin *supra* note 25, at 1204–06 (explaining that if terms are salient to buyers, then sellers—even monopolists—would have a financial incentive to provide them). Platforms may still be discouraged from voluntarily educating users about copyright licensing policies because of the problem of free riding. See *id.* at 1241 (“[A] threshold problem with this premise is that in many situations no seller will have a sufficient incentive to invest in such an advertising campaign, even if the market currently supplies an inefficient term. In a perfectly competitive market, all sellers stand to benefit to the same degree from an attribute becoming salient to buyers, thus causing sellers to replace an inefficient combination of attribute and price with an efficient combination. In this circumstance, advertising is a public good, and no seller will wish to pay the cost of providing it.”).

227. For an overview see Hacothen & Menell, *supra* note 47.

228. See, e.g., HARRISX, Inaugural Tech Media Telecom Pulse Survey 2018, http://harrisx.com/wp-content/uploads/2018/04/Inaugural-TMT-Pulse-Survey_-20-Apr-Final.pdf?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top-stories (finding that 84% of the public favor holding social media platform legally responsible for the content posted); see also THE ECONOMIST, *Facebook Faces a Reputational Meltdown* (Mar. 22, 2018), https://www.economist.com/news/leaders/21739151-how-it-and-wider-industry-should-respond-facebook-faces-reputational-meltdown?cid1=cust/ednew/n/bl/n/20180322n/owned/n/n/nwl/n/n/NA/107979/n&utm_source=newsletter&utm_medium=email&utm_campaign=Editors_Picks&utm_term=20180322 (last visited Mar. 22, 2018); Mark Zuckerberg *In His Own Words: The CNN interview* (Mar. 21, 2018), <http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview-transcript/index.html> (last visited Mar 22, 2018); Jackie Wattles, *Mark Zuckerberg and Facebook under fire from politicians over data controversy*, CNN BUSINESS (Mar. 18, 2018), <http://money.cnn.com/2018/03/18/technology/business/mark-zuckerberg-facebook-politicians->

a reputational meltdown, platforms began adopting self-regulatory measures that far exceeded what the law mandated at that time.²²⁹ For example, leading platforms began censoring political content and imposing mandatory disclosure requirements on advertisers even without being compelled to by law.²³⁰

In a similar vein, public pressure coming from UGC-educated users might push social media platforms to provide stronger copyright protection for user content. For example, our survey's findings indicate that social media users care most about having a right of attribution in their UGC.²³¹ The attribution right is recognized in many foreign jurisdictions but not in the United States for UGC.²³² Nevertheless, with sufficient public pressure, social media platforms might be motivated to develop new technological measures that will safeguard user attribution in attempt to remain attractive.²³³

Some platforms already show efforts to scale down their grossly overbroad licensing policies. Consider LinkedIn as a test case. Until June 2017, LinkedIn's UGC licensing terms were among the worst in the industry. LinkedIn's previous terms mandated that "[LinkedIn retains the right] to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered . . . without any further consent, notice and/or compensation."²³⁴ Cynically enough, LinkedIn's old terms plainly stated to their users that "[a]ny information you submit to us is at your own risk of loss."²³⁵

data/index.html (last visited Mar. 20, 2018) ("The growing scrutiny comes after news broke that Cambridge Analytica, a data firm with ties to President Donald Trump's campaign, reportedly gained access to information about 50 million Facebook (FB) users.").

229. See *supra* note 219.

230. See Nellie Bowles & Sheera Frenkel, *Facebook and Twitter Plan New Ways to Regulate Political Ads*, N.Y. TIMES (May 24, 2018), <https://www.nytimes.com/2018/05/24/technology/twitter-political-ad-restrictions.html> (last visited June 9, 2018); Jack Nicas, *Facebook to Require Verified Identities for Future Political Ads*, N.Y. TIMES (April 6, 2018), <https://www.nytimes.com/2018/04/06/business/facebook-verification-ads.html> (last visited Jun 9, 2018); Julia Angwin & Jeff Larson, *Help Us Monitor Political Ads Online*, PROPUBLICA (Sep. 7, 2017), <https://www.propublica.org/article/help-us-monitor-political-ads-online> (last visited June 9, 2018).

231. See *supra* note 164.

232. See *supra* note 7.

233. One such solution can rely on existing technical systems geared to automatically identify the owner of the copyright in content sharing platforms such as Content ID. See *supra* note 180; see also Elazari Bar On, *supra* note 25, at 612–14; Bamberger, Egelman, Han, Elazari Bar On & Reyes, *supra* note 36, at 140 (proposing a technical solution to empower users' rights with respect to boilerplate terms).

234. *LinkedIn Old Agreement*, *supra* note 4. LinkedIn changed these ToS in June 7, 2017.

235. *LinkedIn Old Agreement*, *supra* note 4.

In June 2017, however, LinkedIn voluntarily backed away from these overbroad contractual provisions to become the poster child for excellence in drafting a balanced ToS agreement that respects users' rights.²³⁶ LinkedIn's updated ToS has several compelling features in them. First, LinkedIn adopted language that substantially narrows its UGC licensing policy. In its revised terms, for example, LinkedIn provides:

[LinkedIn] will not include your content in advertisements for the products and services of third parties to others without your separate consent (including sponsored content) . . . and [w]hile [LinkedIn] may edit and make formatting changes to your content (such as translating it, modifying the size, layout or file type or removing metadata), [they] will not modify the meaning of your expression.²³⁷

Second, similarly to Tumblr and Pinterest, LinkedIn provided its users with a short and simplified version of its terms. Third, and most appealingly, LinkedIn created an animated instructional video that clearly and briefly communicates to users the gist of the platform's UGC licensing policy.²³⁸ LinkedIn's ToS transformation may indicate that social media platforms are already facing public pressure to improve ToS agreements.

B. SUBSTANTIVE REGULATION

Some put faith in enhanced disclosure and education, while others are less optimistic. For instance, a substantial body of literature cautions that social media platforms are becoming so prominent in the digital economy that consumer pressure alone cannot police platforms' behavior.²³⁹ Even if users

236. LinkedIn, *User Agreement*, (effective on Jan. 6, 2020), <https://www.linkedin.com/legal/user-agreement> (hereinafter *LinkedIn Jan. 2020 Agreement*); see also LinkedIn, *User Agreement, Who owns your content? You do*, <https://www.youtube.com/watch?v=ha7ASaPnjbA> (last visited Feb. 26, 2020).

237. *LinkedIn Jan. 2020 Agreement*, *supra* note 234. LinkedIn is not alone in this. Tumblr's ToS, for example, provide that, "[t]he rights you grant in this license are for the limited purposes of allowing Tumblr to operate the Services in accordance with their functionality, improve the Services, and develop new Services. The reference in this license to 'creat[ing] derivative works' is not intended to give Tumblr a right to make substantive editorial changes or derivations." Tumblr, *Tumblr Terms of Service* <https://www.tumblr.com/policy/en/terms-of-service> (last visited Feb. 26, 2020).

238. LinkedIn, *User Agreement, Who owns your content? You do*, *supra* note 236.

239. See, e.g., TIM WU, *THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE* (2018); Stucke, *supra* note 133, at 289 ("[N]otice-and-consent regime is meaningless when bargaining power is so unequal that users do not have a viable alternative option."); Sabeel K. Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 *GEO. L. TECH. REV.* 234, 240 (2018) (emphasis added) (noting that in the modern-day internet economy, "technology companies often rely on murky and opaque terms of service that include various unreasonable provisions, particularly those that allow for arbitrary cutoffs or

care about UGC policies, such terms may not become salient because users are a captive audience—they cannot decide to not participate in the platforms’ services.²⁴⁰ Drawing on this concern, commenters in the privacy arena have urged substantial regulatory oversight to improve terms’ quality.²⁴¹ Our findings suggest that comparable regulatory oversight may also be needed for UGC terms—specifically, a regulatory regime focusing on making copyright terms more salient to users. This would protect users and promote the policies underlying the intellectual property laws governing those terms.²⁴²

Indeed, abusive contractual provisions are uniquely concerning in the UGC arena given the constitutional gravity and broad social implications of copyright policies.²⁴³ Copyright, under the predominant utilitarian approach in the United States, is vested in creators to incentivize creativity and to benefit

invasions of user privacy; and crucially, that all this takes place in a context *where one’s access to and ability to function on these platforms are increasingly necessary for modern economic and social activity*”); Hildebrandt, *supra* note 133, at 253 (“The concern regarding platforms centers around their potential for monopolistic or totalitarian behavior. The lack of viable competitors not only disturbs the supposedly beneficial operations of a free market, it also exposes the users of such platforms to potentially monopolistic governance, leading them to accept terms of service across a number of services which leave these users vulnerable to unwarranted exposure and manipulation.”). For views on how to regulate social media, see *supra* note 23.

240. *Cf.* Korobkin, *supra* note 25, at 1212 (emphasizing that “[e]ven when the seller is a monopolist, buyers have the option of not purchasing the goods or services in question.”); *see also supra* note 211 (explaining the relationship between terms’ salience and unconscionability). For example, in March 2016, the German competition authority scrutinized Facebook for possible abuse of its market powers by inappropriate data collection from its users. *Bundeskartellamt Initiates Proceeding Against Facebook on Suspicion of Having Abused Its Market Power by Infringing Data Protection Rules*, (Mar. 2, 2016), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Meldungen%20News%20Karussell/2016/02_03_2016_Facebook.html. The logic underling that prosecution was that given that Facebook control the market for social media, users have no valid contractual alternatives. *See* Eliana Garcés & Daniel Fanaras, *Antitrust, Privacy, and Digital Platform’s use of Big Data: A Brief Overview*, 28 (1) THE JOURNAL OF THE ANTITRUST, UNFAIR COMPETITION, AND PRIVACY LAW SECTION OF THE CALIFORNIA LAWYERS ASSOCIATION, 23, 32 (2018) (“The implicit assumption is that users’ lack of alternatives to Facebook leads them to accept unfavorable terms they would otherwise not accept.”)

241. *See generally* Bamberger, Egelman, Han, Elazari Bar On & Reyes, *supra* note 36.

242. Such endeavor will complement the rich corpus of legal literature exploring the interaction between private ordering mechanisms such as boilerplate language, technological enforcement and copyright. *See, e.g.*, Elazari Bar On, *supra* note 25; Niva Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*, 12 BERKELEY TECH. L.J. 93 (1997); RADIN, *supra* note 78; and Niva Elkin-Koren, *A Public Regarding Approach to Contracting Copyrights*, in EXPANDING THE BOUNDARIES OF INTELLECTUAL PROPERTY: INNOVATION POLICY FOR THE KNOWLEDGE SOCIETY 191 (Rochelle Dreyfuss et al. eds., 2001).

243. U.S. CONST. art. I, § 8, cl. 8; *see also* Elazari Bar On, *supra* note 25, at 586–614, 668–71.

all of society.²⁴⁴ Overbroad assignment of copyrights in boilerplate UGC licenses without meaningful user consent and on a massive scale might undermine users' protected property rights and impair the incentives for users (and other parties) to engage in future creation, thereby frustrating the utilitarian goals of copyright law.²⁴⁵ In this case, since the adherent, agreeing to the licensing terms, is the creator of the work and the original copyright owner (an adherent-creator), the terms' nonsalient nature exacerbates the problem from an intellectual property perspective.²⁴⁶

244. See, e.g., Robert D Cooter & Uri Y Hacoen, *Progress in the Useful Arts: Foundations of Patent Law in Growth Economics*, 22 YALE J.L. & TECH. 191, 194 n.10 (2020), <https://yjolt.org/progress-useful-arts-foundations-patent-law-growth-economics> (last visited Oct 12, 2020) (citing sources supporting the notion that intellectual property rights are founded on a utilitarian philosophy); see also Christopher Buccafusco & Jonathan Masur, *Intellectual Property Law and the Promotion of Welfare*, COASE-SANDOR WORKING PAPER SERIES IN LAW AND ECONOMICS, No. 790 (2017). This is, of course, not the only philosophical approach to copyright. For a comprehensive discussion on the manner in which boilerplate terms might undermine copyright policies under various conceptions of copyright (such as Lockean, personhood, dialogical, and utilitarian), see Elazari Bar On, *supra* note 25, at 670–73; see also Elkin-Koren, *supra* note 242.

245. Courts have long addressed in their analysis of boilerplate terms the potential implications for public policy interests, not just under the predominate “public policy exception” doctrine and unconscionability standard-form contract law analysis, see Elazari Bar On, *supra* note 25, but in other contexts too, such as legal preemption analysis. *Id.* at 619. As one court stated with respect to the enforceability of statutory waivers, “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.” *Loop, LLC v. Loop 101, LLC*, 236 Ariz. 410, 412 (citations and internal quotations omitted); see also *DeBerard Properties, Ltd. v. Lim*, 20 Cal. 4th 659, 668–69 (June 3, 1999) (citations and internal quotations omitted) (“[A] party may waive a statutory provision if a statute does not prohibit doing so, 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.”).

246. See Elazari Bar On, *supra* note 25, at 591 (explaining the distinction between adherent-creators and adherent-users in the context of judicial intervention in IP-related boilerplate terms, and the distinction’s normative relevance in the context of IP rights assignment in boilerplate). As Elazari explains, 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. The drafter owns nothing, yet seeks to assign or regulate the rights of the adherent in his creations. *Id.* Elazari further explains that adherent-creator contracts have received less attention in IP scholarship than EULAs, in which the drafter owns the IP. *Id.* at 584. 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. *Id.* at 591. As Elazari explains, the rise of UGC and resulting expansion of “adherent-generated content” mandates theoretical adaptations from both an IP and standard form contract perspective. *Id.* at 585. These adaptations are needed to address the adherent-creator versus adherent-user distinction and the rise of adherent-creator contracts. *Id.* at 586. She proposes that since these types of contracts create different externalities from an IP public

Regulators can achieve substantive oversight either *ex ante*, through legislation, or *ex post*, through litigation.²⁴⁷ In the privacy sphere, new ambitious legislative initiatives—notably the GDPR—attempt to address nonsaliency concerns by requiring companies to provide sufficient information about privacy policies to ensure that users’ consent to data sharing is meaningful.²⁴⁸ Similar legislation could address concerns of nonsaliency in the UGC licensing sphere.

A lesson may be taken from the recently enacted Consumer Review Fairness Act of 2016 (CRF).²⁴⁹ This CRF Act was enacted to deter sellers from engaging in the nefarious yet increasingly popular trend of including boilerplate provisions in contracts accompanying the sale of products and services. These provisions require consumers to surrender their copyrights in future reviews of products or services.²⁵⁰ With their consumer-assigned copyrights, sellers could threaten legal actions to prevent consumers from publishing negative reviews criticizing their products or services.²⁵¹ The CRF Act specifically outlaws such practices by voiding “anti-review” and “non-disparagement”

policy perspective, the nature of the contract can be considered as a part of the substantive unconscionability analysis that needs to account for displacement of IP policies under each of these scenarios. *Id.* at 591–92, 670, 674.

247. *Cf.* Korobkin, *supra* note 25, at 1203–06 (2003).

248. *See* Articles 4(11), 7(2) and Recitals 32 and 42 to the GDPR. *See very generally*, European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf; Proposed Regulations under the CCPA, § 999.305(a)(3), available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf>. (“If the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.”).

249. Consumer Review Fairness Act of 2016, H.R. 5111, 114th Congress (2015–2016) codified at 15 U.S.C. § 45b(a).

250. *See id.* at § (2)(b)(1)(c) (rendering contracts with such provisions invalid). Even before the enactment of the law, some courts voided these terms as unconscionable. *See, e.g., Lee v. Makhnevich*, 2013 U.S. Dist. LEXIS 43760 at 4 (S.D.N.Y. Mar. 27, 2013).

251. In the notorious *Medical Justice* case, around 2,000 healthcare providers used boilerplate “anti-review” clauses to either completely ban consumer reviews or assign the copyrights in future consumer reviews written by patients so the healthcare providers would be able to initiate a DMCA takedown notice if and when such reviews were published. *See generally* Eric Goldman, *Understanding the Consumer Review Fairness Act of 2016*, 24 MICH. TELECOMM. & TECH. L. REV. 1, 2–3 (2017); *see also Lee v. Makhnevich*, No. 11 Civ. 8665 PAC, 2013 WL 1234829 (S.D.N.Y. Mar. 27, 2013).

terms.²⁵² Similar legislation could target overbroad copyright assignments in UGC.²⁵³

Legislation could at least compel platforms to provide more meaningful notice to users about UGC policies.²⁵⁴ Several studies in the privacy arena, for example, documented that contextualized disclosure policies improve term salience.²⁵⁵ In a recent study, for example, one author (Elazari) and Professors

252. See 15 U.S.C. § 45b(b); Goldman, *supra* note 251, at 4–6; see also Clay Calvert, *Gag Clauses and the Right to Gripe: The Consumer Review Fairness Act of 2016 & State Efforts to Protect Online Reviews from Contractual Censorship*, 24 WIDENER L. REV. 203, 222–25 (2018); Lucille M. Ponte, *Protecting Brand Image or Gaming the System? Consumer “Gag” Contracts in an Age of Crowdsourced Ratings and Reviews*, 7 WM. & MARY BUS. L. REV. 59, 132–34 (2016).

253. Cf. 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 (1999) (offering to codify a public policy exception in the proposed reform to the Uniform Commercial Code, Article 2B that did not materialize and warning that without such exception the drafters of non-negotiable terms could undermine the goals of intellectual property policies).

254. Cf. Hacothen & Menell, *supra* note 47 (discussing the need to disclosure legislation to improve transparency in the realm of influencer marketing).

255. Many studies, for example, have shown that the disclosure’s type, context, and timing all change consumers’ perception of privacy. See, e.g., John, Acquisti, & Loewenstein, *supra* note 215, at 858–59 (2011) (presenting four studies supporting the proposition that privacy preference changes in different disclosure contexts—for example if the website looked professional versus unprofessional, thereby elevating disclosure risk); Hazim Almuhammedi et al., *Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging*, 6 PROCS. 33RD ANN. ACM. CONF. ON HUM. FACTORS IN COMPUTING SYSS. 787 (2015) (providing real-time information about how lax app data sharing practices prompted over half of studied users to change permissions); see also Rebecca Balebako, et al., *The Impact of Timing on the Salience of Smartphone App Privacy Notices*, PROCS 5TH. ANN. ACM. CCS WORKSHOP ON SECURITY & PRIVACY IN SMARTPHONES & MOBILE DEVICES 63 (2015) (showing that in-app dialogs increase salience more than those shown before an app’s installation); Idris Adjerid, et al., *Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency*, PROCS. NINTH SYMP. ON USABLE PRIVACY & SECURITY 2 (2013) (showing that even a 15-second delay between data use disclosures and the relevant decision can generate measurable differences in privacy-protective behavior). For more discussion about term complexity and the value of simplified disclosures in the privacy arena see Janice Y Tsai, Lorrie Cranor, Serge Egelman & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYSTEMS RESEARCH 254 (2011) (showing that understanding privacy information changes users’ decisions about website use); Ewa Luger, Stuart Moran, & Tom Rodden, *Consent for All: Revealing the Hidden Complexity of Terms and Conditions*, 2013 PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 2687 (advocating for term simplicity); Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist & Joy Zhang, *Expectation and Purpose: Understanding Users’ Mental Models of Mobile App Privacy through Crowdsourcing*, 2012 PROCEEDINGS OF THE ACM INTERNATIONAL CONFERENCE ON PERVASIVE & UBIQUITOUS COMPUTING 501 (highlight the value of educating users about the purpose of privacy terms); Matthew Kay & Michael Terry, *Textured Agreements: Re-envisioning Electronic Consent*, 2010 PROCEEDINGS OF THE SIXTH SYMPOSIUM ON

Kenneth Bamberger, Serge Egelman, Catherine Han, and Irwin Reyes showed that, before being primed to consider privacy, only 1% of their study's respondents mentioned privacy as something they would expect to differ in paid and free versions of an app.²⁵⁶ When asked directly about the issue, however, over half of the respondents believed there would be a difference.²⁵⁷ In light of these and comparable findings, legislators should compel social media platforms to improve their default disclosure designs. For example, platforms could be compelled to provide users with simplified disclosures of UGC licensing policies right before users upload content.²⁵⁸

Even without designated legislative solutions, established contract and unfair competition law could be configured to address users' unmeaningful consent. For example, the Federal Trade Commission (FTC), in pursuit of its broad statutory authority under Section 5 of the FTC Act, could scrutinize and outlaw overbroad copyright boilerplate assignments by deeming them "unfair or deceptive."²⁵⁹ In the privacy context, Professors Daniel Solove and Woodrow Hartzog have suggested that the FTC should expand its enforcement agenda from targeting only explicit contractual violations to targeting a broader range of behaviors that have a deceptive impact, accounting

USABLE PRIVACY AND SECURITY (SOUPS) 1 (showing benefit of improved terms' visual design); Patrick Gage Kelley, Lucian Cesca, Joanna Bresee & Lorrie Faith Cranor, *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, 2010 PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1573 (suggest improving privacy notice through labeling).

256. Bamberger et al., *supra* note 36, at 361.

257. *Id.*

258. To the extent that users are truly a "captive audience," such relaxed measures will certainly be insufficient. Nevertheless, such measures may serve to reduce the frequency or thoughtlessness of users' sharing habits. Indeed, several policymakers have argued that platforms should intentionally introduce so-called "friction" into their services, namely to allow users time to better ponder and evaluate their sharing habits instead of operating as automatons. *See, e.g.*, House of Commons Digital, Culture, Media and Sport Committee, Disinformation and 'Fake News': Final Report Eighth Report of Session 2017–19, at 86 ("Friction can be incorporated into the system, to give people time to think about what they are writing and what they are sharing and to give them the ability to limit the time they spend online; there should be obstacles put in their place to make the process of posting or sharing more thoughtful or slower."). In a similar vein, The Center for Humane Technology suggested simple methods for individuals to adopt in order to introduce friction into their mobile device usage habits. These methods include turning off all notifications, apart from people; changing the color of the screen to 'grayscale,' thereby reducing the intensity and lure of bright colors; keeping home screen to tools only; launching apps by typing; charging devices outside people's bedrooms; removing social media from mobile devices; and telephoning instead of texting. Take Control, <https://www.humanetech.com/take-control> (last visited Oct 18, 2020).

259. 15 U.S.C. § 45(a)(1) (declaring unlawful "unfair or deceptive acts or practices in or affecting commerce").

for users' real-world conceptions and expectations.²⁶⁰ Our findings suggest that existing UGC licensing policies have such a deceptive impact because most users are broadly ignorant and falsely optimistic with respect to them. This alone may justify oversight by the FTC.

Alternatively, state law doctrines—notably the contractual doctrine of unconscionability—could be adjusted to curtail abusive copyright licensing practices.²⁶¹ The doctrine of unconscionability empowers courts to void abusive terms in form contracts that are “shock[ing] to the conscience”²⁶² or unreasonably undermine “the consumer’s benefit from the bargain.”²⁶³ Despite its potential to deter platforms from including overbroad copyright assignments in their ToS, however, the unconscionability doctrine has yet to be interpreted by the courts to sufficiently assume such a deterring function.²⁶⁴

260. See Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 667 (2016); see also CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 123–25 (2016) (discussing the way in which the FTC employed consumer surveys to appraise consumers’ understandings of promotional representations); KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 183–96 (2015) (explaining ways in which the FTC tinkers with legal standards to reflect consumer expectations).

261. See Elazari Bar On, *supra* note 25 (urging the application of unconscionability doctrine to boilerplate terms in technology transactions in light of RESTATEMENT OF THE L. CONSUMER CONTS., § 5 notes at 94–95 (AM. L. INST., Tentative Draft 2019), https://www.ali.org/media/filer_public/05/30/053007a1-2b37-4142-b9c3-7a881e847d50/consumer_contracts_-_td_-_online.pdf, which addresses the one-sidedness of a term that unreasonably undermines “the consumer’s benefit from the bargain”). There are also federal-law policies such as preemption or copyright misuse that can be invoked to strike down a contractual term, but these are less relevant to our context. For an overview see Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CALIF. L. REV. 111, 157–58 (1999).

262. *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593, 605–06 (E.D. Pa. 2007) (“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.’”) (citing *Comb v. PayPal, Inc.*, 218 F. Supp. 2d 1165, 1172 (N.D. Cal. 2002)). However, as noted, courts have invoked a higher standard for procedural unconscionability, requiring “oppression” or an “unfair surprise.” Elazari Bar On, *supra* note 25, at 624–25; THE RESTATEMENT OF THE L. CONSUMER CONT., TENTATIVE DRAFT, at 94–95 (AM. LAW INST. 2019), https://www.ali.org/media/filer_public/05/30/053007a1-2b37-4142-b9c3-7a881e847d50/consumer_contracts_-_td_-_online.pdf

263. *Id.* at 77.

264. See Hila Keren, *Guilt-Free Markets? Unconscionability, Conscience, and Emotions*, 16 B.Y.U. L. REV. 427 444–49 (2016) (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,

When faced with the issue in *Song Fi v. Google*, the District Court of the District of Columbia refused to invoke unconscionability for social media platforms' ToS.²⁶⁵ To bolster its decision to dismiss plaintiffs' claim that YouTube's ToS are unconscionable, the court emphasized that by "[h]aving taken advantage of YouTube's free services, [the] Plaintiffs cannot complain that the terms allowing them to do so are unenforceable."²⁶⁶ This statement is perplexing at best. If anything, because platforms provide free services, their incentive to monetize users' content (or data) by making their terms nonsalient, only increases.²⁶⁷

As one of the authors suggested elsewhere, courts should consider empowering the unconscionability doctrine to meet the challenges of intellectual property boilerplates in the digital age (even beyond the realm of platforms' ToS). Courts could do this under the substantive unconscionability prong while considering term salience under the procedural unconscionability prong.²⁶⁸ For example, courts could find boilerplate provisions that undermine statutory copyrights (such as the right to create derivative works) to become *prima facie* unconscionable—thereby shifting the burden to prove otherwise

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 actually be worse-off if contractual terms would be voided since drafters will only draft stricter 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, *supra* note 25; Lemley, *Beyond Preemption*, *supra* note 261, at 163 (noting that "even though Article 2B [of the U.C.C.] 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. The same will undoubtedly continue to be true in Article 2B cases.").

265. *Song Fi, Inc. v. Google Inc.*, 72 F. Supp. 3d 53, 59 (D.D.C. Oct. 29, 2014).

266. *Id.* at 64 (emphasis added). The court reached similar results in *Darnaa, LLC v. Google, Inc.*, 2015 U.S. Dist. LEXIS 161791 (N.D. Cal. Dec. 2, 2015). In *Darnaa*, the plaintiff argued that several provisions of YouTube's ToS, including, *inter alia*, the terms that allow YouTube broad discretion over content removal, were unconscionable. The court found that YouTube's ToS "involve[d] only a marginal degree of procedural unconscionability," and are not so "one-sided as to be substantively unconscionable." *Id.* at 8. Moreover, the court emphasized, in the framework of its 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.*

267. Indeed, as the rich literature in the privacy arena has long-established, the nonsaliency of privacy related terms has provided fertile ground for platforms to draft overbroad terms that enable them to extract users' data far beyond what is needed to maintain their services. See Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606 (2014); see also the review in Bamberger, Egelman, Han, Elazari Bar On, & Reyes *supra* note 36, at 356–57.

268. See Elazari Bar On, *supra* note 25.

to the drafter.²⁶⁹ Alternatively, courts could invigorate the unconscionability doctrine by expanding the doctrine's remedies (for example, by introducing restitution), providing for fee-shifting, or reframing the doctrine from a defense to a cause of action.²⁷⁰ Proposals like these are not foreign to intellectual property policy. Courts, for example, have used fee-shifting to combat copyright and patent misuses for decades.²⁷¹

Finally, databases and technological enforcement can be used to monitor and police the quality of UGC terms in platforms' ToS. Platforms already use technological tools to *enforce* adhesive terms in form contracts (e.g., YouTube Content ID automatically enforces the platform's authority to remove allegedly violating content), so little prevents regulators from employing similar tools. For example, a government agency (such as the FTC) could create a publicly available database of boilerplate terms classified by how much such terms undermine copyright policy.²⁷² At least, such a database would draw attention from consumer advocacy groups and users, which would increase

269. *Id.*

270. See Hazel Glenn Beh, *Contract Law Present and Future: A Symposium to Honor Professor Charles L. Knapp on Fifty Years of Teaching Law: Curing the Infirmities of the Unconscionability Doctrine*, 66 HASTINGS L.J. 1011, 1022–45 (2014). Professor Margaret Radin also considered a potential tort-based solution to which she called “tort of intentional deprivation of basic legal rights.” See Radin, *supra* note 78, at 140.

271. Regarding copyright, see, e.g., *Omega S.A. v. Costco Wholesale Corp.*, 776 F.3d 692, 695–96; see also 17 U.S.C. § 505 (interpreted at *Fogerty v. Fantasy, Inc.*, 510 U.S. 517, 525–26 (1994)) (allowing the court discretion in awarding attorney fees to the prevailing party under certain standards). Regarding patents, see *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, 572 U.S. 545 (2014); Gaia Bernstein, *The Rise of the End User in Patent Litigation*, 55 B.C. L. REV. 1443 (2014); see also in the context of “patent trolls,” *Small v. Implant Direct Mfg. LLC*, 2014 U.S. Dist. LEXIS 154468, *9–10 (S.D.N.Y. Oct. 22, 2014) (citing *Lumen View Tech*, 2014 U.S. Dist. LEXIS 74209, 2014 WL 2440867, at *7 (S.D.N.Y. May 30, 2014) (“[T]he 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.”); *Yufa v. TSI Inc.*, 09-CV-01315-KAW, 2014 U.S. Dist. LEXIS 113148, 2014 WL 4071902, at *4 (N.D. Cal. Aug. 14, 2014) (“Today pursuant to 35 U.S.C. § 285, [t]he court in exceptional cases may award reasonable attorney fees to the prevailing party” (citing *Octane Fitness*, 134 S. Ct. at 1756)). See generally Hannah Jiam, *Fee-shifting and Octane Fitness: An Empirical Approach Toward Understanding “Exceptional”*, 30 BERKELEY TECH. L.J. 611 (2015). One of the authors has similarly suggested using the equitable remedy of restitution to combat patent overreach in the context of pharmaceutical patent overreach. See Uri Y. Hacothen, *Evergreening At Risk*, 33 HARV. J.L. & TECH. 480 (2020).

272. See Elazari Bar On, *supra* note 25, at 686–67; see also RADIN, *supra* note 78. In contrast, the FTC has provided rough guidelines concerning what constitutes adequate disclosure in the case of social media endorsers. The FTC's Endorsement Guides: What People Are Asking, FEDERAL TRADE COMMISSION (2017), <https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking> (last visited Feb. 26, 2020).

term salience.²⁷³ Such a database could also be used to train machine-learning algorithms to highlight and flag suspected terms for review by consumers, regulators, and lawyers.²⁷⁴

V. CONCLUSION

In the digital age, social media platforms have become the primary venues for communicating, creating, interacting, sharing content, and engaging in cultural dialogue. When users join social media platforms and agree to the platforms' ToS, they also agree to license their copyrights to their uploaded creative content. In this study, we documented that the most popular social media platforms employ boilerplate copyright-licensing provisions that are grossly overbroad, unnecessary for the platforms' service operation, and detrimental to users' rights and copyright policy. We put forward the largest and most comprehensive empirical study to date, surveying 1,033 social media users geared to evaluate users' awareness, perceptions, and expectations and—most importantly—term salience (the effect on market decision-making) of these boilerplate copyright-licensing terms. Our findings indicate that a

273. Cf. 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, 91–93 (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, although the law has robust provisions, it does not guarantee consumers will actually make use of such provisions). Michael argues that Israel should adopt the publication of “Guidance” on potentially unconscionable terms that have been subject to previous litigations, similar to the approach taken in the U.K., see *supra* note 223, and a simplified disclosure model where drafters who adopt a term which is “grey listed” will need to separately disclose it in the boilerplate in a meaningful, salient way.

274. Machine learning is being used to spot other abusive bot-initiated behavior such as the spread of fake news or fake endorsements. For example, 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.” Berkeley Engineering, *Fighting Fake News* (Nov. 14, 2018), <https://engineering.berkeley.edu/magazine/fall-2018/fighting-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/> (noting Instagram states they “built machine learning tools to help identify accounts that use [third-party apps for boosting followers] and removing the inauthentic activity”). For an overview of a tool supporting machine learning analysis of privacy policies see 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/> (Polisis, <https://pribot.org/>). For a tool allowing users to search a name of a mobile app and learn about its actual information collection practice see APPCENSUS, <https://appcensus.mobi/> (reviewed in Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpahanah, Narseo Vallina-Rodriguez & Serge Egelman, *Won't Somebody Think of the Children?* “Examining COPPA Compliance at Scale”, 2018 PROCEEDINGS ON PRIVACY ENHANCING TECHS. 63 (developed by one of the author's co-authors on this cited research).

substantial portion of users who share their copyrighted content on social media do not understand and have unrealistic expectations about their rights to their content and the rights they give away. Simultaneously, a substantial portion of users appears to care about their copyrights and assert that they would have changed their social media behavior if they had understood the boilerplate terms. After analyzing our study's findings, we proposed various insights for law and policy—ranging from soft remedial solutions to substantial regulatory oversight.

APPENDIX

A. COMPLETE TEXTUAL ANALYSIS OF PLATFORMS' UGC TERMS

| <i>Platform</i> | <i>Terms</i> | |
|-------------------------------|----------------------------|--|
| Twitter ²⁷⁵ | Perpetuity/ Termination | In all such cases, the Terms shall terminate, including, without limitation, your license to use the Services, except that the following sections shall continue to apply: II, III [License], V, and VI. |
| | 3rd parties | you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to make Content submitted to or through the Services available to other companies, organizations or individuals for the syndication, broadcast, distribution, promotion or publication of such Content on other media and services, subject to our terms and conditions for such Content use. Such . . . uses . . . may be made with no compensation paid to you |
| | Modification | use, copy, reproduce, process, adapt, <u>modify</u> , publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed) You understand that we may modify or adapt your Content as it is distributed, syndicated, published, or broadcast by us and our partners and/or make changes to your Content in order to adapt the Content to different media. |
| | Derivative works | - |
| | Immediate removal | We reserve the right to remove Content alleged to be infringing without prior notice, at our sole discretion, and without liability to you. |

275. Twitter, *Terms of Service*, (May 25, 2018), https://twitter.com/en/tos/previous/version_13.

| <i>Platform</i> | <i>Terms</i> | |
|-------------------------|----------------------------|---|
| | Commercial | this license includes the right for Twitter to provide, <u>promote</u> , and improve the Services and [same for 3rd parties] |
| | Ideas | Any feedback, comments, or suggestions you may provide regarding Twitter, or the Services is entirely voluntary and we will be free to use [it] as we see fit and without any obligation to you. |
| | Moral rights | - |
| | Publicity rights | - |
| Pinterest 276 | Perpetuity/ Termination | <p>Upon termination, you continue to be bound by Sections 2 [license] and 6–12 of these Terms.</p> <p>Nothing in these Terms shall restrict other legal rights Pinterest may have to User Content, for example under other licenses.</p> <p>Following termination or deactivation of your account, or if you remove any User Content from Pinterest, we may retain your User Content for a commercially reasonable period of time for backup, archival, or audit purposes. Furthermore, Pinterest and its users may retain and continue to use, store, display, reproduce, repin, modify, create derivative works, perform, and distribute any of your User Content that other users have stored or shared through Pinterest.</p> |
| | 3rd parties | You grant Pinterest and our users a non-exclusive, royalty-free, transferable, sublicensable, worldwide license |
| | Modification | <p>to use, store, display, reproduce, save, modify . . . perform, and distribute . . . solely for the purposes of operating, developing, providing, and using the Pinterest Products.</p> <p>We reserve the right to remove or modify User Content for any reason, including User Content that we believe violates these Terms or our policies.</p> |

276. Pinterest, *Terms of Service* (effective Nov. 1, 2016), <https://policy.pinterest.com/en/terms-of-service-2016>.

| <i>Platform</i> | <i>Terms</i> | |
|----------------------------|----------------------------|---|
| | Derivative works | create derivative works . . . solely for the purposes of operating, developing, providing, and using the Pinterest Products. Following termination or deactivation of your account, [Pinterest may] continue to . . . create derivative works . . . of your User Content that other users have stored or shared through Pinterest. |
| | Immediate removal | Pinterest may terminate or suspend this license at any time, with or without cause or notice to you. |
| | Commercial | - |
| | Ideas | If you choose to submit comments, ideas or feedback, you agree that we are free to use them without any restriction or compensation to you. |
| | Moral rights | - |
| | Publicity rights | - |
| Vine ²⁷⁷ | Perpetuity/ Termination | the Terms shall terminate, including, without limitation, your license to use the Services, except that the following sections shall continue to apply: 4, 5, 7, 8, 10, 11, and 12. |
| | 3rd parties | with the right to sublicense You agree that this license includes the right for Vine . . . to make Content . . . available to other companies, organizations or individuals who partner with Vine for the syndication, broadcast, distribution or publication of such Content on other media and services, subject to our terms and conditions for such Content use. Such additional uses . . . may be made with no compensation paid to you |
| | Modification | use, copy, reproduce, process, adapt, <u>modify</u> , publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed). |
| | Derivative works | - |
| | Immediate removal | We also retain the right to create limits on use and storage at our sole discretion at any time without prior notice to you. |

277. Vine.co, *Terms Of Service*, (Jan. 21, 2013), <https://www.docracy.com/0am76hh9685/vine-co-terms-of-service-tos>.

| <i>Platform</i> | <i>Terms</i> | |
|------------------------|----------------------------|---|
| | Commercial | you agree that Vine and its parent, third party providers and partners may place such advertising on the Services or in connection with the display of Content or information from the Services whether submitted by you or others. You agree that this license includes the right for Vine to provide, promote, and improve the Services. |
| | Ideas | - |
| | Moral rights | - |
| | Publicity rights | - |
| Snapchat 278 | Perpetuity/ Termination | Regardless of who terminates these Terms, both you and Snap Inc. continue to be bound by Sections 3 [Rights You Grant Us], 6, 9, 10, and 13–22 of the Terms. <i>[for Live, Local, and any other crowd-sourced Services]</i> you also grant us a perpetual license |
| | 3rd parties | <i>[For Services other than Live, Local, or crowd-sourced]</i> you grant. . . a worldwide, royalty-free, sublicensable, and transferable <i>[for Live, Local, and any other crowd-sourced Services]</i> you also grant Snap Inc., our affiliates, and our business partners the unrestricted, worldwide, perpetual right and license to [publicity rights] |

278. Snap Inc., *Snap Inc. Terms of Service*, (effective Jan. 10, 2017), <https://web.archive.org/web/20210101071802/>, <https://snap.com/en-US/terms>). If you live in the United States, Snap’s terms of service effective October 30, 2019 state the following: With respect to your use of Bitmoji, you grant Snap Inc., our affiliates, and our business partners a worldwide, perpetual, royalty-free, sublicensable, and transferable license to host, store, use, display, reproduce, modify, adapt, edit, publish, distribute, promote, exhibit, broadcast, syndicate, publicly perform, and distribute (a) any actual or simulated likeness, image, voice, name, poses, or other personal characteristics (collectively, your “Likeness”) embodied in a Bitmoji Avatar or the Bitmoji Services, and (b) any materials you create using the Bitmoji Services, as well as the right to create and use derivative works from those materials, in any and all media or distribution methods (now known or later developed). This license is for the limited purpose of operating, developing, providing, promoting, and improving the Services and researching and developing new ones. This means, among other things, that you will not be entitled to any compensation from Snap Inc., our affiliates, or our business partners if your name, likeness, or voice is conveyed through or in connection with Bitmoji, either on the Bitmoji application or on one of our business partner’s platforms. Snap Inc., *Terms of Service*, (effective Oct. 30, 2019), <https://www.snap.com/en-US/terms>.

| <i>Platform</i> | <i>Terms</i> | |
|------------------------|----------------------------|--|
| | Modification | [<i>For Services other than Live, Local, or crowd-sourced</i>] license to host, store, use, display, reproduce, <u>modify</u> , <u>adapt</u> , <u>edit</u> , publish, and distribute that content. |
| | Derivative works | [<i>for Live, Local, and any other crowd-sourced Services</i>] license to create derivative works |
| | Immediate removal | [W]e may access, review, screen, and delete your content at any time and for any reason, including . . . if we think your content violates these Terms. |
| | Commercial | advertising may sometimes appear near your content [<i>For Services other than Live, Local, or crowd-sourced</i>] This license is for the limited purpose of operating, developing, providing, <u>promoting</u> , and improving the Services and researching and developing new ones. [<i>for Live, Local, and any other crowd-sourced Services</i>] <u>promote</u> , exhibit, broadcast, syndicate, sublicense, publicly perform, and publicly display [content] in any form and in any and all media or distribution methods (now known or later developed). |
| | Ideas | If you volunteer feedback or suggestions, just know that we can use your ideas without compensating you. |
| | Moral rights | - |
| | Publicity rights | [<i>for Live, Local, and any other crowd-sourced Services</i>] right and license to use your name, likeness, and voice. This means, among other things, that you will not be entitled to any compensation [from Snapchat or third parties]. |
| LinkedIn 279 | Perpetuity/ Termination | You can end this license for specific content by deleting such content from the Services, or generally by closing your account, except (a) to the extent you shared it with others as part of the Service and they copied, re-shared it or stored it and (b) for the reasonable time it takes to remove from backup and other systems. |

| <i>Platform</i> | <i>Terms</i> | |
|-----------------|-------------------|---|
| | 3rd parties | A worldwide, transferable and <u>sublicensable</u> right to use. We will get your consent if we want to give others the right to publish your content beyond the Services. However, if you choose to share your post as "public", we will enable a feature that allows other Members to embed that public post onto third-party services, and we enable search engines to make that public content findable through their services |
| | Modification | copy, <u>modify</u> , While we may edit and make format changes to your content (such as translating or transcribing it, modifying the size, layout or file type or removing metadata), we will not modify the meaning of your expression |
| | Derivative works | - |
| | Immediate removal | We may change, suspend or discontinue any of our Services. . . . We don't promise to store or keep showing any information and content that you've posted. |
| | Commercial | We will not include your content in advertisements for the products and services of third parties to others without your separate consent (including sponsored content). However, we have the right, without payment to you or others, to serve ads near your content and information, and your social actions may be visible and included with ads, as noted in the Privacy Policy |
| | Ideas | By submitting suggestions or other feedback regarding our Services to LinkedIn, you agree that LinkedIn can use and share (but does not have to) such feedback for any purpose without compensation to you |
| | Moral rights | - |
| | Publicity rights | - |

| <i>Platform</i> | <i>Terms</i> | |
|-------------------------|----------------------------|---|
| Instagram 280 | Perpetuity/ Termination | You can end this license anytime by deleting your content or account. However, content will continue to appear if you shared it with others and they have not deleted it. |
| | 3rd parties | you hereby grant to us a non-exclusive, royalty-free, <u>transferable</u> , <u>sub-licensable</u> , worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content |
| | Modification | you hereby grant to us a . . . worldwide license to . . . modify . . . and create derivative works of your content (consistent with your privacy and application settings) |
| | Derivative works | you hereby grant to us a . . . worldwide license to . . . modify . . . and create derivative works of your content (consistent with your privacy and application settings) |
| | Immediate removal | We can remove any content or information you share on the Service if we believe that it violates these Terms of Use, our policies (including our Instagram Community Guidelines), or we are permitted or required to do so by law. We can refuse to provide or stop providing all or part of the Service to you (including terminating or disabling your account) immediately to protect our community or services, or if you create risk or legal exposure for us, violate these Terms of Use or our policies (including our Instagram Community Guidelines), if you repeatedly infringe other people's intellectual property rights, or where we are permitted or required to do so by law. If you believe your account has been terminated in error, or you want to disable or permanently delete your account, consult our Help Center. |

280. Instagram, *Terms of Use*, (revised April 19, 2018), <https://www.facebook.com/help/instagram/termsfuse> (“We do not claim ownership of your content, but you grant us a license to use it. Nothing is changing about your rights in your content. We do not claim ownership of your content that you post on or through the Service. Instead, when you share, post, or upload content that is covered by intellectual property rights (like photos or videos) on or in connection with our Service, you hereby grant to us a non-exclusive, royalty-free, transferable, sub-licensable, worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). You can end this license anytime by deleting your content or account. However, content will continue to appear if you shared it with others and they have not deleted it. To learn more about how we use information, and how to control or delete your content, review the Data Policy and visit the Instagram Help Center.”).

| <i>Platform</i> | <i>Terms</i> | |
|------------------------|----------------------------|--|
| | Commercial | <p>Permission to use your username, profile picture, and information about your relationships and actions with accounts, ads, and sponsored content.</p> <p>You give us permission to show your username, profile picture, and information about your actions (such as likes) or relationships (such as follows) next to or in connection with accounts, ads, offers, and other sponsored content that you follow or engage with that are displayed on Facebook Products, without any compensation to you. For example, we may show that you liked a sponsored post created by a brand that has paid us to display its ads on Instagram. As with actions on other content and follows of other accounts, actions on sponsored content and follows of sponsored accounts can be seen only by people who have permission to see that content or follow. We will also respect your ad settings. You can learn more here about your ad settings.</p> |
| | Ideas | We always appreciate feedback or other suggestions, but may use them without any restrictions or obligation to compensate you for them, and are under no obligation to keep them confidential.. |
| | Moral rights | - |
| | Publicity rights | - |
| Facebook 281 | Perpetuity/ Termination | In all such cases [of termination] this Statement shall terminate, but the following provisions will still apply: 2.2, 2.4 [license], 3–5, 9.3, and 14–18. |
| | 3rd parties | you grant us a non-exclusive, transferable, <u>sub-licensable</u> , <u>royalty-free</u> , worldwide license to use any IP content |
| | Modification | By "use" we mean use, run, copy, publicly perform or display, distribute, modify, translate, and create derivative works of. |
| | Derivative works | By "use" we mean . . . create derivative works of. |
| | Immediate removal | We can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies. |

281. Facebook, *Terms of Service*, (revised Jan. 30, 2015), <https://www.facebook.com/legal/terms/previous>.

| <i>Platform</i> | <i>Terms</i> | |
|-----------------------|----------------------------|---|
| | Commercial | you give us permission to use your name, profile picture, content, and information in connection with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without any compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it. |
| | Ideas | - |
| | Moral rights | - |
| | Publicity rights | - |
| YouTube 282 | Perpetuity/ Termination | The above licenses granted by you in video Content you submit to the Service terminate within a commercially reasonable time after you remove or delete your videos from the Service. You understand and agree, however, that YouTube may retain, but not display, distribute, or perform, server copies of your videos that have been removed or deleted. The above licenses granted by you in user comments you submit are perpetual and irrevocable. |
| | 3rd parties | grant YouTube a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license in connection with the Service and YouTube's (and its successors' and affiliates') business |
| | Modification | - |
| | Derivative works | grant YouTube a worldwide, non-exclusive, royalty-free . . . license to use, reproduce, distribute, prepare derivative works of, display, and perform the Content in connection with the Service and YouTube's (and its successors' and affiliates') business |
| | Immediate removal | YouTube does not permit copyright infringing activities and infringement of intellectual property rights on the Service, and YouTube will remove all Content if properly notified that such Content infringes on another's intellectual property rights. YouTube reserves the right to remove Content without prior notice. |

282. YouTube, *Terms of Service*, (May 25, 2018), <https://www.youtube.com/t/terms?archive=20180525>.

| <i>Platform</i> | <i>Terms</i> | |
|------------------------------|----------------------------|--|
| | Commercial | including without limitation for promoting and redistributing part or all of the Service (and derivative works thereof) in any media formats and through any media channels. |
| | Ideas | - |
| | Moral rights | - |
| | Publicity rights | - |
| Reddit ²⁸³ | Perpetuity/ Termination | you grant us a royalty-free, <u>perpetual</u> , <u>irrevocable</u> , non-exclusive, <u>unrestricted</u> , worldwide license The following sections will survive any termination of these Terms or of your Accounts: 4 (Your Content) |
| | 3rd parties | and to authorize others to do so. |
| | Modification | - |
| | Derivative works | reproduce, prepare <u>derivative works</u> , distribute copies, perform, or publicly display your user content in any medium and |
| | Immediate removal | Without advance notice and at any time, we may, for violations of this agreement or for any other reason we choose: (1) suspend your access to reddit, (2) suspend or terminate Your Account or reddit gold membership, and/or (3) remove any of your User Content from reddit |
| | Commercial | for any purpose, including commercial purposes |
| | Ideas | [<i>under new terms</i>] |
| | Moral rights | [<i>under new terms</i>] |

283. Reddit, *supra* note 4; Reddit, *supra* note 7. Reddit revised its ToS on September 15, 2020: Reddit no longer requires a license for *any* commercial use. Here are further additions: (1) Reddit broadened the license to include: “Your Content and any name, username, voice, or likeness provided in connection with Your Content.” (2) This license includes the right for us to make Your Content available for syndication, broadcast, distribution, or publication by other companies, organizations, or individuals who partner with Reddit. You also agree that we may remove metadata associated with Your Content. (3) you irrevocably waive any claims and assertions of moral rights or attribution with respect to Your Content. (4) Any ideas, suggestions, and feedback about Reddit or our Services that you provide to us are entirely voluntary, and you agree that Reddit may use such ideas, suggestions, and feedback without compensation or obligation to you. Reddit, *Reddit User Agreement*, (effective Oct. 15, 2020), <https://www.redditinc.com/policies/user-agreement-october-15-2020>.

| <i>Platform</i> | <i>Terms</i> | |
|-----------------------------|----------------------------|--|
| | Publicity rights | [<i>under new terms</i>] |
| Vimeo ²⁸⁴ | Perpetuity/ Termination | Upon termination, all licenses granted by Vimeo will terminate. Sections 6 and 11 though [sic] 16 shall survive termination. |
| | 3rd parties | you grant Vimeo and its affiliates a limited, worldwide, non-exclusive, royalty-free license and right to |
| | Modification | - |
| | Derivative works | copy, transmit, distribute, publicly perform and display (through all media now known or hereafter created), and <u>make derivative works from your video</u> for the purpose of (i) displaying the video within the Vimeo Service; (ii) displaying the video on third party websites and applications through a video embed or Vimeo's API subject to your video privacy choices; (iii) allowing other users to play, download, and embed on third party websites the video, subject to your video privacy choices; (iv) promoting the Vimeo Service, provided that you have made the video publicly available; and (v) archiving or preserving the video for disputes, legal proceedings, or investigations. |
| | Immediate removal | Vimeo may suspend, disable, or delete your account (or any part thereof) or block or remove any content you submitted if Vimeo determines that you have violated any provision of this Agreement or that your conduct or content would tend to damage Vimeo's reputation and goodwill. |
| | Commercial | (iv) promoting the Vimeo Service, provided that you have made the video publicly available |
| | Ideas | Vimeo shall have the right to use your suggestions without any compensation to you. |
| | Moral rights | you waive any so-called "moral rights" in your non-video content. |

284. You grant Vimeo permission to use your name, likeness, biography, trademarks, logos, or other identifiers used by you in your account profile for the purpose of displaying such properties to the public or the audiences you have specified. You may revoke the foregoing permission by deleting your account. Vimeo shall have the right to identify public profiles in its marketing and investor materials. Vimeo, *Terms of Service Agreement* (effective Oct. 6, 2017), <https://web.archive.org/web/20190201171914/>, <https://vimeo.com/terms>. These terms changed on June 26, 2019.

| <i>Platform</i> | <i>Terms</i> | |
|------------------------------|----------------------------|--|
| | Publicity rights | - |
| Tumblr ²⁸⁵ | Perpetuity/ Termination | this license to your Subscriber Content continues even if you stop using the Services, primarily because of the social nature of Content shared through Tumblr's Services you acknowledge and agree that: (a) deleted Subscriber Content may persist in caches or backups for a reasonable period of time and (b) copies of or references to the Subscriber Content may not be entirely removed (due to the nature of reblogging, for example). |
| | 3rd parties | you grant Tumblr a non-exclusive, worldwide, royalty-free, sublicensable, transferable right and license |
| | Modification | modify, adapt (including, without limitation, in order to conform it to the requirements of any networks, devices, services, or media through which the Services are available) |
| | Derivative works | and create derivative works of, such Subscriber Content. The rights you grant in this license are for the limited purposes of allowing Tumblr to operate the Services in accordance with their functionality, improve and promote the Services, and develop new Services. The reference in this license to "creat[ing] derivative works" is not intended to give Tumblr a right to make substantive editorial changes or derivations, but does, for example, enable reblogging, which allows Tumblr Subscribers to redistribute Subscriber Content from one Tumblr blog to another in a manner that allows them to add their own text or other Content before or after your Subscriber Content. |
| | Immediate removal | Tumblr may change, suspend, or discontinue any or all of the Services at any time, including the availability of any product, feature, database, or Content (as defined below). |
| | Commercial | The rights you grant in this license are for the limited purposes of . . . promot[ing] the Services |

285. Github, *tumblr/policy*, (May 9, 2018), <https://github.com/tumblr/policy/commit/7ad5058c9ff20d57d7f4ce7d5f0fd2f32a05cab#> (providing Tumblr's ToS).

| <i>Platform</i> | <i>Terms</i> | |
|-----------------|------------------|---|
| | Ideas | - |
| | Moral rights | - |
| | Publicity rights | - |

B. SURVEY

1. **Consent**

2. **Screening**

- 1) Have you once uploaded your work to at least one of the following platforms: Facebook, Instagram, YouTube, Twitter, Snapchat, LinkedIn, Vimeo, Reddit, Pinterest, Tumblr, Vine?
- Yes
 - No

3. **Demographic quotas**

- 1) Have you once uploaded your work to at least one of the following platforms: Facebook, Instagram, YouTube, Twitter, Snapchat, LinkedIn, Vimeo, Reddit, Pinterest, Tumblr, Vine?
- Yes
 - No
- 2) Have you once uploaded your work to at least one of the following platforms: Facebook, Instagram, YouTube, Twitter, Snapchat, LinkedIn, Vimeo, Reddit, Pinterest, Tumblr, Vine?
- Yes
 - No
- 3) What is your gender?
- Male
 - Female
 - Other
- 4) What is your age? (you must be above 18 year old to take this survey)
- Under 18
 - 18 to 24
 - 25 to 34
 - 35 to 44

- 45 to 54
 - 55 to 64
 - 65 or older
- 5) What is the highest degree or level of school you have completed?
- High school graduate—high school diploma or the equivalent (for example: GED)
 - Bachelor's degree (for example: BA, AB, BS)
 - Master's degree
 - Professional degree or doctorate degree (for example: MD, DDS, DVM, LLB, JD, PhD, EdD)
- 6) What was your annual household income in 2017?
- Less than \$15,000
 - \$15,000 to under \$25,000
 - \$25,000 to under \$50,000
 - \$50,000 to under \$75,000
 - \$75,000 to under \$100,000
 - \$100,000 to under \$150,000
 - Over \$150,000

4. Definitions

- 1) **“Work” or “Content”** means copyright-protected content **created by you**. Content such as art, poetry, prose, photographs, sound and musical compositions, illustrations, video, or audiovisual works.
- 2) If we generally say **“Platform” or “social media platform,”** we mean: Facebook, Instagram, YouTube, Twitter, Snapchat, LinkedIn, Vimeo, Reddit, Pinterest, Vine.
- 3) **“Use”** means: Publicly display, copy, reproduce, distribute, perform, or transmit the work.²⁸⁶
- 4) **“Terms”** means: The platforms terms-of-use, or the contract that requires you to click “I Accept” when you join the platform.

5. Social media index

286. This definition was based on the findings of the copyright boilerplate landscape analysis, described in Section III(B)(1).

- 1) Do you receive any direct income from sharing or uploading content (created by you) to social media platforms?
 - Yes
 - No

- 2) Do you receive any value from sharing or uploading content (created by you) to social media platforms?
 - Yes, direct income
 - Yes, promoting or marketing myself, my work or my business
 - Getting my work out there
 - I use social media platforms for social interaction only

- 3) Considering these options, how often do you upload content (created by you) onto social media platforms?
 - Once a day or more
 - Once a week
 - Once a month
 - Once every couple months

6. Awareness

- 1) Mark all the platforms you are using (uploading content to) [you can choose multiple options]
 - Facebook
 - Instagram
 - YouTube
 - Twitter
 - Snapchat
 - LinkedIn
 - Vimeo
 - Reddit
 - Pinterest
 - Vine

- 2) For <Platform chosen by the participant>, mark one option for each statement—According to its terms:
 - <Platform may> Grant others (third parties) license to use my work.
 - <Platform may> Modify my work.
 - <Platform may> Create new works based on my work.
 - <Platform may> Use my work for any commercial purpose.
 - <Platform may> Remove content upon their sole discretion.

- *<Platform may>* Display my work indefinitely, even if I delete my account.
- *<Platform may>* Place advertisement on my work.
- *<Platform may>* Use my work to promote the platform services.
- *<Platform may>* Display my work until I delete my account.

7. Expectations

- 1) ***<Immediate removal>*** In your opinion sharing platforms should be allowed to [mark to most appropriate option]:
 - Remove content they determine, upon their sole discretion, that violates their terms
 - Remove content for any reason
 - Remove content only they are required to do so under law
 - None of the above.
- 2) ***<Commercial (and other) uses>*** In your opinion, social media platforms should be able to [mark all that apply]:
 - Use, display or distribute my work only for the purpose of the platform's function (social communication).
 - Use, display or distribute my work for the purpose to promote the platform or the platform service.
 - Use, display or distribute my work for any purpose, including commercial use.
 - Use, display or distribute my work for the purpose of training artificial intelligence algorithms (machine learning).
 - None of the above.
- 3) ***<display and distribution>*** In your opinion, a platform should be able to [mark one option]:
 - Display and distribute my work only on the platform.
 - Display and distribute my work on any means of communication.
 - None of the above.
- 4) ***<display and distribution—third parties>*** In your opinion, who should be allowed to display and distribute your work? [mark all relevant options]:
 - The platform.
 - Its users.

- Other parties, at the discretion of the platform.
 - No-one.
- 5) <**Termination**> In your opinion, display and distribution of your work should be available [mark one option]:
- Only for as long as I maintain an account on the platform.
 - Only for as long as I agree.
 - Only until I chose to remove my work.
 - Indefinitely.

8. Understanding:

- 1) When a platform mentions in its terms that “you waive your so-called moral rights” it means [mark all that apply]:
- I will not be paid any royalties [incorrect]
 - It can present my work without name
 - I wave all the copyrights in my work.
 - It can change the meaning of my work and distort it in a manner which is disrespectful.
 - I don’t know what “moral rights” are.
- 2) When a platform mentions in its terms that “you grant the platform a license to prepare derivative work” it means that [choose one option]:
- I grant a perpetual (permanent) license to all the rights I have in my work.
 - I allow the platform to copy and share my work.
 - I allow the platform to place advertisements on my work without my consent.
 - I allow the platform to create new versions of my work.
 - None of the above

9. Salience

- 1) Consider the following scale <*Extremely likely, likely, neither likely nor unlikely, unlikely, extremely unlikely*> and indicate how likely you are to use such platform:
- Only uses your work for the purpose of operating its platform and nothing else.
 - Associate your name with your work.
 - Uses your work for training AI algorithms (machine learning)
 - Can remove your content for any reason

- Under its terms, allows to use your work for any purpose including commercial use.
 - Under its terms, authorizes others (non-users) to distribute and modify your work.
 - Under its terms, can create new works that are based on your work.
 - Under its terms, say you cannot change your mind and cancel the license (permission) you grant the platform to use/display your work.
 - Under its terms, allows to display ads on your work.
 - Under its terms, allows to present your work without naming you as the creator.
 - Under its terms, allows to modify your work (for any purpose, not just when technically required).
- 2) The following statement represent varies [sic] Intellectual Property rights. Please rank them according to their importance to you (with 1 being the most important and 7 the least important).
- The meaning or from of my work won't be altered in a manner that is disrespectful without my consent.
 - My work must be displayed/associated with my name.
 - My work won't be significantly modified (unless technically required) without my consent.
 - My work won't be associated with ads.
 - My work won't be used for commercial purposes, without my consent.
 - The platform won't be able to authorize other parties (non-users) to use (display and distribute) my work without my consent.
 - I am able to change or cancel the license (permission) I give platforms to use my work if I change my mind.

C. TERM AWARENESS ACROSS PLATFORMS

| The platform may: | Facebook | | | Instagram | | | YouTube | | | Twitter | | |
|---|----------|-------|-------|-----------|-------|-------|---------|-------|-------|---------|-------|-------|
| | Yes | No | D/K | Yes | No | D/K | Yes | No | D/K | Yes | No | D/K |
| Grant others (third parties) license to use my work | 19.9% | 46.2% | 33.9% | 22.2% | 47.1% | 30.8% | 24.2% | 47.5% | 28.3% | 20.2% | 48.1% | 31.7% |
| Modify my work | 18.2% | 51.3% | 30.5% | 23.2% | 47.7% | 29.0% | 26.5% | 50.1% | 23.4% | 20.0% | 53.7% | 26.3% |
| Create new works based on my work | 24.9% | 40.7% | 34.4% | 26.7% | 41.3% | 32.0% | 28.9% | 39.0% | 32.1% | 24.6% | 42.7% | 32.7% |
| Use my work for any commercial purpose | 28.2% | 40.3% | 31.5% | 30.8% | 38.1% | 31.2% | 35.8% | 37.0% | 27.1% | 27.9% | 41.4% | 30.7% |
| Remove content upon their sole discretion | 84.6% | 6.5% | 8.9% | 77.2% | 11.2% | 11.6% | 87.3% | 6.3% | 6.3% | 79.5% | 8.7% | 11.8% |
| Display my work indefinitely, even if I delete my account | 32.7% | 33.7% | 33.7% | 32.7% | 36.8% | 30.5% | 32.5% | 37.8% | 29.7% | 28.4% | 39.1% | 32.5% |
| Place advertisement on my work | 43.1% | 27.7% | 29.3% | 37.6% | 30.3% | 32.0% | 75.6% | 11.7% | 12.7% | 46.3% | 27.1% | 26.6% |
| Use my work to promote the platform services | 36.3% | 31.3% | 32.4% | 40.0% | 29.5% | 30.5% | 51.7% | 23.0% | 25.4% | 41.9% | 27.4% | 30.7% |
| Display my work until I delete my account | 58.8% | 14.5% | 26.7% | 62.2% | 14.6% | 23.2% | 65.9% | 14.9% | 19.2% | 61.9% | 16.9% | 21.2% |

| The platform may: | Snapchat | | | LinkedIn | | | Vimeo | | |
|---|----------|-------|-------|----------|-------|-------|-------|-------|-------|
| | Yes | No | D/K | Yes | No | D/K | Yes | No | D/K |
| Grant others (third parties) license to use my work | 27.2% | 38.0% | 34.9% | 17.2% | 52.3% | 30.5% | 30.8% | 46.2% | 23.1% |
| Modify my work | 19.5% | 48.7% | 31.8% | 15.6% | 54.7% | 29.7% | 23.1% | 53.9% | 23.1% |
| Create new works based on my work | 22.6% | 39.5% | 38.0% | 18.0% | 45.3% | 36.7% | 34.6% | 42.3% | 23.1% |
| Use my work for any commercial purpose | 25.1% | 37.4% | 37.4% | 22.7% | 43.0% | 34.4% | 42.3% | 34.6% | 23.1% |
| Remove content upon their sole discretion | 69.7% | 14.4% | 15.9% | 68.8% | 16.4% | 14.8% | 76.9% | 15.4% | 7.7% |
| Display my work indefinitely, even if I delete my account | 24.6% | 43.1% | 32.3% | 24.2% | 46.1% | 29.7% | 38.5% | 38.5% | 23.1% |
| Place advertisement on my work | 36.9% | 31.8% | 31.3% | 36.7% | 30.5% | 32.8% | 80.8% | 11.5% | 7.7% |
| Use my work to promote the platform services | 31.8% | 31.8% | 36.4% | 32.0% | 31.3% | 36.7% | 34.6% | 46.2% | 19.2% |
| Display my work until I delete my account | 42.6% | 33.3% | 24.1% | 62.5% | 14.8% | 22.7% | 65.4% | 15.4% | 19.2% |

| The platform may: | Reddit | | | Pinterest | | | Vine | | |
|---|--------|-------|-------|-----------|-------|-------|-------|-------|--------|
| | Yes | No | D/K | Yes | No | D/K | Yes | No | D/K |
| Grant others (third parties) license to use my work | 18.0% | 46.8% | 35.3% | 23.6% | 40.5% | 35.9% | 0.0% | 33.3% | 66.7% |
| Modify my work | 24.8% | 47.5% | 27.8% | 20.3% | 45.6% | 34.2% | 66.7% | 0.0% | 33.3% |
| Create new works based on my work | 24.1% | 39.7% | 36.3% | 26.2% | 39.2% | 34.6% | 0.0% | 33.3% | 66.7% |
| Use my work for any commercial purpose | 27.8% | 37.3% | 34.9% | 32.5% | 33.8% | 33.8% | 0.0% | 33.3% | 66.7% |
| Remove content upon their sole discretion | 81.7% | 7.5% | 10.9% | 79.8% | 8.0% | 12.2% | 0.0% | 33.3% | 66.7% |
| Display my work indefinitely, even if I delete my account | 46.8% | 28.8% | 24.4% | 38.0% | 26.6% | 35.4% | 33.3% | 33.3% | 33.3% |
| Place advertisement on my work | 48.5% | 25.8% | 25.8% | 40.5% | 27.9% | 31.7% | 66.7% | 0.0% | 33.3% |
| Use my work to promote the platform services | 39.0% | 25.8% | 35.3% | 41.8% | 26.2% | 32.1% | 0.0% | 0.0% | 100.0% |
| Display my work until I delete my account | 53.9% | 20.0% | 26.1% | 64.1% | 11.0% | 24.9% | 33.3% | 0.0% | 66.7% |

D. TERMS' SALIENCE (RANKING)

The following statements represent various Intellectual Property rights. Please rank them according to their importance to you (with 1 being the most important and 7 the least important):

