

37:2 BERKELEY TECHNOLOGY LAW JOURNAL

2022

Pages

623

to

936

Berkeley Technology Law Journal

Volume 37, Number 2

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

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

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

Copyright © 2022 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 37

NUMBER 2

2022

TABLE OF CONTENTS

ARTICLES

THE TRANSNATIONAL DATA GOVERNANCE PROBLEM	623
<i>Douglas W. Arner, Giuliano G. Castellano & Eriks K. Selga</i>	
POLICING POLICE TECH: A SOFT LAW SOLUTION	701
<i>Barry Friedman, Farhang Heydari, Max Isaacs & Katie Kinsey</i>	
A USER'S GUIDE TO SECTION 230, AND A LEGISLATOR'S GUIDE TO AMENDING IT (OR NOT).....	757
<i>Jeff Kosseff</i>	
THE DYSTOPIAN RIGHT OF PUBLICITY	801
<i>Dustin Marlan</i>	
TRADEMARK CONFUSION SIMPLIFIED: A NEW FRAMEWORK FOR MULTIFACTOR TESTS	865
<i>Daryl Lim</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 37 BERKELEY TECH. L.J. ____ (2022).

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

2021–2022

Executive Board

Editors-in-Chief
NATALIE T. CRAWFORD
LOC HO

Managing Editor
MIN JUNG "MJ" HAN

Senior Scholarship Editor
GRACE MCFEE

Senior Articles Editors
SHALEV NETANEL
DAKOTA SNEED
SOPHIA WALLACH

Senior Student Publication Editors
MEET MEHTA
RACHEL PAIGE THOMPSON

Senior Executive Editor
RACHEL WILSON

Senior Production Editor
ROBIN CHANG

Senior Online Content Editor
KARNIK HAJJAR
THOMAS HORN

Editorial Board

Submissions Editors
TIFFANY ALLEN
CONNOR KENNEDY
BARBARA ROWINSKA

Member Relations Editors
RYAN CAMPBELL
AL MALECHA

Web & Technology Editors
HENRY METRO
KATHERINE WANG

Student Publication Editors
JOSH CAYETANO
JENNIFER CHUNG
CHANTEL JOHNSON

RICH ABIDOR
ALLISON BLAKE
JONATHAN CHACON
LUCILLE DAI-HE
RUTUJA DESHPANDE

Production Editors
KEATON BLAZER
SARAH DAVIDSON
JOELLE FERGUSON
HANNA KIM

Notes & Comments Editors
PAULINE LE
THOMAS MATTES

Podcast Editors
SETH BERTOLUCCI
ISABEL JONES

Alumni Relations Editors
CHRIS MUSACHIO
CARESSA TSAI

Articles Editors
ROBERT FAIRBANKS
KURT FREDRICKSON
KHASH GOSHTASBI
DYLAN HOULE
JESSICA LI

Technical Editors
REBECCA HO
JOSEPH KINGERSKI

Symposium Editors
JOANNA LEUNG
PEYTEN SHARP

Commentaries Editors
CLINTON EWELL
ISABELLA PESTANA

External Relations Editor
SALMA FIKRAT

LLM Editor
JOSH LEE KOK THONG

JUSTINE MCCARTHY POTTER
BREANNA QIN
EVA SPITZEN
JESSICA WANG
ALI ZARRABI

MEMBERSHIP

Vol. 37 No. 2

Associate Editors

OGAN AKTOLUN	PAYTON FONG	SAMI MOACDIEH
HAZIM ALWAZIR	GAL FORER	CHRIS MUSACHIO
AKHIL BHARDWAJ	JONATHAN GIBSON	CAIO NUNES
HARSH BORA	JOYCE GUO	DANI O'DONNELL
ABRAHAM BRAUNER	KIANA HARKEMA	ELIZABETH OH
MARIANA CAMACHO	ROGER KAI	SUBASH RENGASAMY
SHIH-WEI CHAO	BRITTA KAJIMURA	NIKKI SEICHEPINE
ZHONGREN CHENG	KEVIN KALLET	ANUJA SHAH
SURITI CHOWDHARY	WILL KASPER	PEYTEN SHARP
NOAH COHEN	JUNG KIM	ANDREA SOTELO
ZACH COUGER	HUNTER KOLON	GASPERI
KAVYA DASARI	ALEXANDRA KUTSCHERA	YUNG WAN
BRIGITTE DESNOES	JIM LISCHESKE	YUHAN WU
RAPHAEL DIONIS	PRIMAVERA MARTINEZ	MENGTING XU
MATHEUS DRUMMOND	VASUNDHARA MAJITHIA	CASSIE YIN
MARTIN FISCHER		ROBERT ZHU

Members

VRINDA AGARWAL	ADRIAN GEILEN	DEVANSHI PATEL
NATASYA AMALIA	MATTHEW GEORGY	MAXIME PEREZ
RAIVO ANDRIAN	VARTIKA GOYAL	ADNAN PERWEZ
JOHN BATOHA	BELINDA GRUNFELD	DUSTIN POORE
BEN BROKESH	JENNIFER JEONG	MAYA PRASAD
HANNAH BROWN	VINCENT JORALEMON	ADAM PUKIER
EMMA BURKE	ABHA KASHYAP	RAKSHITH RAJESH
JOSHUA CAYETANO	AROHI KASHYAP	DARSHINI RAMIAH
MATTHEW CHA	NATHANIEL KELLERER	SUMEDH RISHI
JAEOUNG CHOI	SONALI KHANNA	KERMIT RODRIGUEZ
NUTTANID CHOKRUNGVARANON	HUNTER KOLON	IAN SMITH
GABBY CIRELLI	THANAVIT KOOCHINGCHAI	ALI SUEBERT
MACKENZIE CONCEPCION	MARIAN LEE	MEGHAN SULLIVAN
BRANDON DAILEY	CAROLINE LESTER	AISHWARYA TODALBAGI
LIVIA DOMENIG	SHUANG LIU	CARESSA TSAI
MADÉLINE ELKINS	MATTHEW LUEVANO	JOHNATHAN VAKNIN
SUMMER ELLIOT	CHIAGOZIEM MARK ANEKE	NICK VESCIO-FRANZ
JACOBO ENRIQUE RUEDA FERNANDEZ	GARRETH MCCRUDDEN	RUCHIKA WADHAWAN
JUSTIN FAN	ROSS MOODY	RAGHAV WADHWA
CITRA FATIHAH	KOJI MORIKAWA	DANIELLA WENGER
KAYLA FEDLER	DYLAN MOSES	TED WESENBERG
KAESHA FREYALDENHOVEN	LAWRENCE MYUNG	MENGTING XU
MARIANA GARCIA BARRAGAN	MIRANDA PAEZ	RUIKAI YAN
	CHLOE PAN	Ji Yu
	GAYATRI PARANJAPE	ANDY ZACHRICH
		JIawei ZHANG

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 2021–2022

Executive Director

WAYNE STACY

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

ROBERT BARR	RAMYA CHANDRASEKHAR
KATHRYN HASHIMOTO	YUAN HAO

Staff

MARK COHEN	RICHARD FISK
NATALIE COLETTA	IRYS SCHENKER
JANN DUDLEY	ALLISON SCHMITT

THE TRANSNATIONAL DATA GOVERNANCE PROBLEM

Douglas W. Arner,[†] Giuliano G. Castellano^{††} & Eriks K. Selga^{†††}

ABSTRACT

The historical paradigm of data globalization is shattering. Fragmentation of transnational data flows and related governance frameworks is emerging globally as the result of fundamental differences in the governance mechanisms progressively deployed by the major economies and standard-setting jurisdictions to control the digital world. The irreconcilable positions of the United States, the European Union, and the People’s Republic of China—further heightened by technological competition and geopolitical tension—are breaking down the global data economy and threaten to fracture its core infrastructure, the internet.

In this Article, we provide a systematic framework to analyze this emerging global landscape and assess its implications. Our analysis shows that each jurisdiction is characterized by an evolving and distinct data governance style based on its attitude towards markets and governance, the normative principles supporting the exercise of control over data, and the mode of regulating data. As these domestic governance styles consolidate into competing and conflicting data governance regimes, their transnational export and impact are fracturing the existing transnational data governance paradigm, which is based on free data movement, and hindering international coordination in the global data economy. We characterize this dynamic as the wicked problem of transnational data governance, which no single solution can address.

The Article highlights three approaches to address this wicked problem: (1) a bilateral approach that draws from the riparian system for water rights; (2) a plurilateral approach allowing the free circulation of data within sector-specific regulatory coalitions; (3) a multilateral approach, entailing either a hard law structure, with a “Digital Bretton Woods,” or a soft law “Digital Stability Board.” The implementation of a combination of these approaches offers a basis for a workable foundation for transnational data governance that harnesses the benefits of data globalization without undermining domestic sovereign priorities.

DOI: <https://doi.org/10.15779/Z38GF0MX5G>

© 2022 Douglas W. Arner, Giuliano G. Castellano, Eriks K. Selga

[†] Kerry Holdings Professor in Law, RGC Senior Fellow in Digital Finance and Sustainable Development, Associate Director, HKU-Standard Chartered FinTech Academy, and Senior Fellow, Asia Global Institute, University of Hong Kong; Senior Visiting Fellow, University of Melbourne.

^{††} Associate Professor in Law, and Deputy Director, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong.

^{†††} Research Fellow, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong.

Douglas W. Arner gratefully acknowledges the financial support of the Hong Kong Research Grants Council Senior Research Fellowship Scheme and the Qatar National Research Fund. Giuliano G. Castellano thanks the Hong Kong Research Grant Council for generous support through the General Research Fund (GRF n. 17607119).

TABLE OF CONTENTS

I.	INTRODUCTION	624
II.	EVOLUTION OF TRANSNATIONAL DATA GOVERNANCE AND DATA GOVERNANCE STYLES.....	635
III.	FRAGMENTATION OF TRANSNATIONAL DATA GOVERNANCE: SOVEREIGNTY, COMPETITION, AND SECURITIZATION	660
A.	DIGITAL SOVEREIGNTY.....	660
1.	<i>Emerging Concepts</i>	663
2.	<i>Divergent Scopes</i>	665
B.	EXTRATERRITORIALIZATION AND INTERNALIZATION	669
C.	DATA SECURITIZATION	673
D.	THE END OF THE INTERNET AS A GLOBAL COMMONS?	676
1.	<i>A Multi-Centered Internet</i>	678
2.	<i>Data Infrastructure Conflicts</i>	679
IV.	ADDRESSING THE WICKED PROBLEM OF TRANSNATIONAL DATA GOVERNANCE.....	683
A.	THE WICKED PROBLEM OF TRANSNATIONAL DATA GOVERNANCE	684
B.	BILATERAL APPROACHES: THE RIPARIAN STATUS QUO.....	687
C.	PLURILATERAL APPROACHES: REGULATORY COALITIONS.....	690
D.	MULTILATERAL APPROACHES: A NEW (DIGITAL) BRETTON WOODS.....	692
V.	A PATH FORWARD?	696

I. INTRODUCTION

Data permeates all aspects of modern economies and societies. As a result of decades of digitalization, data in digital form¹ are routinely created, gathered,

1. Data is the representation of information, concepts, and other phenomena in different (analog or digital) forms and mediums so that they are suitable for communication, interpretation, and processing by human beings or automated systems. *See generally* Chaim Zins, *Conceptual Approaches for Defining Data, Information, and Knowledge*, 58 J. AM. SOC'Y FOR INFO. SCI. & TECH. 479, 480 (2007) (exploring the foundations of information science and formulating

and shared across the globe to support core societal functions, including healthcare systems, transportation, international commerce, and national security. Digitalization brings together two interrelated processes: digitization, the transformation of analog information into digital form, and datafication, the application of quantitative and other analytics to data.² The “digitization of everything”³ and the unprecedented expansion of datafication have led jurisdictions to acquire ever-expanding amounts of data, setting the stage for a new economy and the Fourth Industrial Revolution.⁴ Thus, data is becoming a strategic asset that interlocks individuals, private actors, and public entities in global networks. Such a complex digital structure not only supports traditional economic activities but also gives rise to a new economic ecosystem (the data economy) where measurable information is sourced, analyzed, aggregated, and exchanged.⁵

definitions for data, information, and knowledge). In this paper, we refer to data in the digital format.

2. See VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, *BIG DATA*, 78 (2013) (defining digitization as “the process of converting analog information into zeros and ones of binary code so computers can handle it” and noting that “to datify a phenomenon is to put it in a quantified format to it can be tabulated and analyzed”). On the concept of datafication, see also Ulises A. Mejias & Nick Couldry, *Datafication*, 8 *INTERNET POL’Y REV.*, 1 (2019) (defining datafication as the quantification of human life through digital information and, thus, noting that data increasingly interfaces with human behavior).

3. The “digitization of everything” generally refers to the wide and systematic transformation of any input—from music to biometric—into machine-readable electronic signal. This process is a step change, since it allows leverage on exponential computing power and, therefore, it is an agent of profound socio-economic changes. See KLAUS SCHWAB, *THE FOURTH INDUSTRIAL REVOLUTION*, 9 (2017) (noting that “technology and digitization will revolutionize everything.”).

4. The development of infrastructure and technologies leveraging on and supporting data flows, together with digitization, are central dynamics characterizing the Fourth Industrial Revolution. See SCHWAB, *supra* note 3, at 12 (positing that the Fourth Industrial Revolution (2000-present) is characterized by mobile internet, sensors, actuators, machine learning, and artificial intelligence).

5. See generally Alexander Trauth-Goik, *Repudiating the Fourth Industrial Revolution Discourse: A New Episteme of Technological Progress*, *WORLD FUTURES* 55, 55-78 (2020) (presenting the growing interdependency of society and data, and suggesting a need for new ethical frameworks); SCHWAB, *supra* note 3; Albert Opher, Alex Chou, Andrew Onda & Krishna Sounderrajan, *The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization-A Perspective for Chief Digital Officers and Chief Technology Officers*, IBM (Mar. 13, 2016), https://hosteddocs.ittoolbox.com/rise_data_econ.pdf (discussing the emergence of a data economy based on the transformation of data into a strategic asset).

Societal dependence on data is an irreversible phenomenon, magnified by the diffusion of new technologies—such as the Internet of Things (IoT), distributed ledger technology (DLT), and artificial intelligence (AI)—and accelerated by the COVID-19 pandemic.⁶ Data has therefore drawn comparisons to the most valuable resources in the world, including oil, oxygen, and water.⁷ Like the counterparts of these analogies, national and international policymakers increasingly prioritize control over data, perhaps as *the* strategic priority, internationally and domestically. As framed by *The Economist* in 2017: “The world’s most valuable resource is no longer oil, but data.”⁸ Put differently, data has become “the new oil.”⁹

Over the past three decades, a techno-libertarian ethos has dominated transnational data governance, which is reflected in the free movement of data across the decentralized infrastructure of the internet. Absent an international legal framework governing data, domestic policymakers are developing different systems of rules and processes to extend their domestic and international jurisdictional control over the digital world. Policymakers are

6. LAURA DENARDIS, *THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH* 4 (2020) (outlining the growing dependence of society on data in day-to-day functions). On the role of technology in the context of the COVID-19 pandemic, see generally Douglas W. Arner, Ross P. Buckley, Andrew M. Dahdal & Dirk A. Zetsche, *Digital Finance, COVID-19 and Existential Sustainability Crises: Setting the Agenda for the 2020s* (Univ. Hong Kong Fac. L. Rsch. Paper No. 2021/001), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3783605 (examining how technology can help resolve the COVID-19 crisis at a micro and macro level); Douglas W. Arner, Janos Nathan Barberis, Julia Walker, Ross P. Buckley, Andrew M. Dahdal & Dirk A. Zetsche, *Digital Finance & The COVID-19 Crisis* (Univ. Hong Kong Fac. L. Rsch. Paper 2020/017, Mar. 26, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3558889 (highlighting how the digitization of financial services may help address the challenges emerging from the COVID-19 crisis).

7. For data analogies, see generally Dennis D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, 66 ME. L. REV. 373 (2013) (examining the development of data discussion following the emergence of new analogies); Jakob Svensson & Oriol Poveda Guillén, *What is Data and What Can It Be Used For? Key Questions in the Age of Burgeoning Data-Essentialism*, 2 J. DIGIT. SOC. RSCH. 65 (2020) (examining various data analogies and comparing them to actual data utility); Francesca Casalini & Javier López González, *Trade and Cross-Border Data Flows*, OECD TRADE POLICY PAPERS, No. 220 (2019) (examining the impact of data on trade and vice versa); R. J. ANDREWS, *INFO WE TRUST: HOW TO INSPIRE THE WORLD WITH DATA* 1–40 (2019) (comparing data to water, as it can be stored for later use).

8. *The World’s Most Valuable Resource is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (highlighting the rise in value of data).

9. *Data is Giving Rise to a New Economy*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy> (presenting an argument for the growing importance of data and how it impacts data policy).

developing legal and regulatory frameworks to define rights and obligations for data holders and consumers;¹⁰ competition policies have been triggered to curb data abuse by dominant incumbent firms;¹¹ and new rules to assert control over internal and external data flows and related infrastructure are being enacted.¹² Crucially, as these data governance frameworks develop and expand their reach across policy domains, they create new fault lines for geopolitical tensions and strategic competition centered around priorities like digital innovation, competitiveness, and cybersecurity. The urge for state actors to assert their sovereignty over data lies at the heart of these initiatives.¹³ The result is the emergence of a global data governance framework that is transnational in nature and increasingly fragmented¹⁴ by design.

10. Rights and obligations for data stakeholders extends across many policy domains. *See generally* Rene Abraham, Johannes Schneider & Jan vom Brocke, *Data governance: A conceptual framework, structured review, and research agenda*, 49 INT'L J. INFO. MGMT. 424, 424–38 (2019) (highlighting the evolving state of data governance across domains, within data science, and in organizational scopes); Larry Catá Backer, *And an Algorithm to Entangle them All? Social Credit, Data Driven Governance, and Legal Entanglement in Post-Law Legal Orders*, in ENTANGLED LEGALITIES: BEYOND THE STATE 79 (Nico Krish ed., 2022)/// (arguing that the emergence of data driven analytics and algorithmic techniques is reshaping the conception of data governance).

11. For instance, the FTC recently filed a complaint against Facebook in an ongoing federal antitrust case, alleging that Facebook resorted to illegal buy-or-develop schemes to maintain market dominance. *See* Press Release, Fed. Trade Comm'n, FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate (Aug. 19, 2021), <https://www.ftc.gov/news-events/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush>.

12. *See infra* Section III.A for a discussion on digital sovereignty and the territorialization of internal and external data flows.

13. OECD, THE PATH TO BECOMING A DATA-DRIVEN PUBLIC SECTOR (2019); U.N. SECRETARY-GENERAL, DATA STRATEGY OF THE SECRETARY-GENERAL FOR ACTION BY EVERYONE, EVERYWHERE (May 2020) https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf (recognizing the rise of data as a strategic asset around the world and presenting a framework for jurisdictions to mobilize and secure data capabilities).

14. Originally birthed in public international law, fragmentation has been used to refer to the tendency for legal rules and regulatory provisions to develop across different sectorial axes in an uncoordinated fashion both within and across jurisdictions. *See generally* INT'L L. COMM'N, FRAGMENTATION OF INTERNATIONAL LAW: DIFFICULTIES ARISING FROM THE DIVERSIFICATION AND EXPANSION OF INTERNATIONAL LAW: REPORT STUDY GROUP ON THE FRAGMENTATION OF INTERNATIONAL LAW, at 10-28 U.N. Doc. A/CN.4/L.682 (2006) (providing an exhaustive analysis of the notion of “fragmentation of international law”); Eyal Benvenisti & George W. Downs, *The Empire's New Clothes: Political Economy and the Fragmentation of International Law*, 60 STAN. L. REV. 595 (2007); Martti Koskenniemi, *Fragmentation of International Law? Postmodern Anxieties*, 15 LEIDEN J. INT'L L. 553 (2002). In the context of

This Article advances a twofold argument to identify the challenge of transnational data governance. First, we posit that fragmentation stems from the emergence of distinct data governance styles in the three largest economies: the United States, the European Union, and China. The multiplication of domestic regulatory initiatives may appear to be the result of piecemeal reforms. However, drawing from the literature of “varieties of capitalism,”¹⁵ regulatory governance, and modes of regulation,¹⁶ we demonstrate that the approaches adopted in each jurisdiction reflect patterns of specific cultural, political, economic, and legal characteristics.¹⁷

sectoral fragmentation, see Giuliano G. Castellano & Andrea Tosato, *Commercial Law Intersections*, 72 HASTINGS L.J., 999 (2021) (positing that the fragmentation of commercial law results in the emergence of systems of rules and principles that when come into contact give rise to a phenomenon termed “commercial law intersections”); Joshua Karton, *Sectoral Fragmentation in Transnational Contract Law*, 21 U. PA. J. BUS. L. 142 (2018) (describing how commercial law has split across sectorial lines both at domestic and international level).

15. The notion of “varieties of capitalism” was introduced by Peter Hall and David Soskice to analyze the institutional differences between “liberal market economies” and “coordinated market economies” in different socio-economic ambits. See PETER A. HALL & DAVID SOSKICE, *VARIETIES OF CAPITALISM* 8-20 (2001) (introducing two core types of capitalism—liberal and coordinated—and noting that liberal market economies are more apt to support radical innovation whereas coordinated market economies tend to support incremental innovation). The notion has been further developed and applied in different contexts. See, e.g., Gregory Shaffer, *Governing the Interface of U.S.-China Trade Relations*, 115 AM. J. INT’L L. 622 (2021) (explaining the differences between capitalist models in the United States and China in the context of international trade relationships). See also BEYOND VARIETIES OF CAPITALISM: CONFLICT, CONTRADICTIONS, AND COMPLEMENTARITIES IN THE EUROPEAN ECONOMY (Bob Hancké, Martin Rhodes, and Mark Thatcher, eds., 2007) (offering an overview of the application of the varieties of capitalism and a critique in the European context).

16. Robert A. Kagan, *How Much Do National Styles of Law Matter?*, in *REGULATORY ENCOUNTERS: MULTINATIONAL CORPORATIONS AND AMERICAN ADVERSARIAL LEGALISM*, 1-30 (Robert A. Kagan & Lee Axelrad eds., 2002) (discussing implications of different national and regulatory systems); Julia Black, *Learning from Regulatory Disasters*, 10 POL’Y Q. 3 (2014) (introducing regulatory governance as a form of managing risks to achieve a publicly stated objective); see generally Giuliano G. Castellano, Alain Jeunmaître & Bettina Lange, *Reforming European Union Financial Regulation: Thinking through Governance Models*, 23 EUR. BUS. L. REV. 409 (2012) (typifying the relationship between the institutional setting and the mode of regulation in the context of regulatory models in the EU).

17. For the notion of “regulatory styles,” see generally Francesca Bignami & R. Daniel Kelemen, *Kagan’s Atlantic Crossing: Adversarial Legalism, Eurolegalism, And Cooperative Legalism*, in *VARIETIES OF LEGAL ORDER: THE POLITICS OF ADVERSARIAL AND BUREAUCRATIC LEGALISM* (Jeb Barnes & Thomas F. Burke eds., 2017) (defining regulatory styles as making, crafting, and implementing laws and regulations, conducting litigation, adjudicating disputes, and using courts); Cary Coglianese & Robert A. Kagan, *Regulation and regulatory processes* in *REGULATION AND REGULATORY PROCESSES* (Cary Coglianese & Robert A. Kagan eds., 2007) (presenting an overview of characteristics of regulatory styles, including statutory design,

Historically, the United States has followed a laissez-faire approach to data and technology. This model, epitomized by Silicon Valley's technology champions—Google, Apple, Facebook/Meta, Amazon, Microsoft (GAFAM)—has nurtured the rise of the internet in its current paradigm: globalized, permissionless, and supportive of free trade.¹⁸ Upon the blueprint offered by the Washington Consensus, the internet developed favoring minimal regulation over data and fostering a frictionless pro-business environment for transnational data flows.¹⁹

Owing to the evolving priorities and conflicting interests of major jurisdictions, the traditional transnational data governance paradigm is shattering. The increasing extension of sovereignty over data and networks by policymakers in China, the European Union, and the United States and the emergence of distinct governance styles at the domestic level result in a marked territorialization of data, thus irreversibly altering the laissez-faire status quo that has supported global data flow in the past two decades. The invasion of Ukraine in February 2022 has heightened existing geopolitical tensions fueling these conflictual dynamics.

In all three jurisdictions, data governance represents a central strategic priority. In the United States, the 2019 Federal Data Strategy encompasses a ten-year vision for leveraging data in policymaking, a paradigmatic shift towards data centralization in support of competitiveness and national security.²⁰ In the European Union, policy efforts have aimed at protecting both the rights of E.U. citizens and the free circulation of data within its “Single Market.”²¹ With the implementation of the General Data Protection

characteristics of regulated entities, and background political environment). We refer to data governance styles as the variables characterizing approaches to the policy and regulatory domain, involving private and public actors.

18. See *infra* Section II.B for a discussion on U.S. data governance styles.

19. Dani Rodrik, *Goodbye Washington Consensus, Hello Washington Confusion? A Review of the World Bank's Economic Growth in the 1990s: Learning from a Decade of Reform*, 44 J. ECON. LITERATURE 973 (2006) (arguing for a paradigmatic end to the dominating Washington Consensus, which was the international development mantra of “stabilizing, privatizing, and liberalizing” rules favoring the free-market models of the U.S.).

20. Amy O'Hara, *US Federal Data Policy: An Update on The Federal Data Strategy and The Evidence Act*, 5 INT'L J. POPULATION DATA SCI. 1, 1-15 (2020) (presenting how the Federal Data Strategy expresses a growing priority for federal agencies to collect and process data).

21. Brett Aho & Roberta Duffield, *Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China*, 49 ECON. & SOC'Y 187, 188-92 (2020) (outlining how the European

Regulation (GDPR) in 2016,²² Brussels marked a major shift in its governance style. The GDPR, in fact, extends beyond the borders of the European Union, expanding its influence to the digital domain.²³ The European Union’s 2020 Data Strategy aims to harmonize cross-border data flows and data sharing between its twenty-seven countries, both to protect core E.U. interests and support competitiveness, particularly vis-à-vis large technology companies—Big Tech—in the United States and China.²⁴ As extraterritoriality rules and adequacy standards apply to regulate the flow of data outside the Single Market, more jurisdictions are now adopting E.U. standards—a “Brussels effect.”²⁵

China’s strategic approach aims at pursuing a broader developmental agenda. As large technology-intensive firms—such as Baidu, Alibaba, and Tencent (BATs)—have emerged as alternatives to GAFAM, technology has become a key component within the economic and social policies pursued by Beijing. The 2017 Cybersecurity Law²⁶ and the new Data Security Law and Personal Information Protection Law (PIPL),²⁷ both adopted in 2021, as

Union has adopted consumer and privacy-protection oriented regulation to counter growing data-surveillance architecture).

22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) /1.

23. See generally ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020) (arguing that the European Union is competing with other governance styles through opt-in rules to access its market).

24. Big Tech generally refers to the leading global tech companies. However, legislators are currently trying to define the boundaries of what makes Big Tech. See generally VALERIE C. BRANNON, CONG. RSCH. SERV., LSB10309, REGULATING BIG TECH: LEGAL IMPLICATIONS 1 (Sept. 11, 2019) (highlighting how legislators are using the amount of monthly users to define Big Tech, such as companies with “more than 30 million active monthly users in the U.S., more than 300 million active monthly users worldwide, or who have more than \$500 million in global annual revenue”); Aho & Duffield, *supra* note 21 (outlining how the European Union has adopted consumer and privacy-protection oriented regulation to counter growing data-surveillance architecture).

25. See *infra* Section II.C for a discussion on the “Brussels effect.”

26. Huárén míngònghéguó wǎngluò ānquán fǎ (中华人民共和国网络安全法)(现行有效) [Cybersecurity Law of the People’s Republic of China] (promulgated by the Standing Comm. Nat’l People’s Cong., Nov. 7, 2016, effective June 1, 2017) 2016 P.R.C. Laws (China), translated in Rogier Creemers, Graham Webster & Paul Triolo, DIGICHINA: STANFORD UNIVERSITY (June 28, 2018), <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> [hereinafter PRC Cybersecurity Law].

27. Zhōnghuá rén míngònghéguó shùjù ānquán fǎ (中华人民共和国数据安全法)

highlighted by the release of a new State Council strategy²⁸ in August 2021, are central components of its 14th Five-Year Plan (2021–25),²⁹ in which technology is instrumental to both national security and socio-economic development, with a new focus on centralization and perhaps even autarky.³⁰ At the global level, a “Beijing effect” is taking shape in the form of a growing number of jurisdictions relying on technological and governance solutions developed in China.³¹ As a result of this, Chinese digital influence has extended to the global market, challenging the U.S. incumbent position (under the Washington Consensus or the “California effect”) and competing with the E.U. efforts to affirm domestic values in the global landscape.³²

Second, we argue that emerging data governance regimes are on a collision course that is poised to compromise globalization and the global data

[Data Security Law of the People’s Republic of China] (promulgated by the Standing Comm. Nat’l People’s Cong. June 10, 2021, effective Sept. 1, 2021) 2021 P.R.C. Laws (China), *translated in DIGICHINA: STANFORD UNIVERSITY* (June 29, 2021), <https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/> [hereinafter PRC Data Security Law]; Zhōnghuá rén míngònghéguó gèrén xīnxi bǎohù fǎ (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People’s Republic of China] (promulgated by the Standing Comm. of Nat’l People’s Cong. Aug. 20, 2021, effective Nov. 1, 2021), 2021 P.R.C. Laws (China), *translated in DIGICHINA: STANFORD UNIVERSITY* (Aug. 20, 2021), <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> [hereinafter PRC Personal Information Protection Law].

28. The Central Committee of the Communist Party of China and the State Council issued the “Implementation Outline for the Construction of a Government Ruled by Law (2021-2025),” XINHUA NEWS AGENCY (Aug. 11, 2021), xinhuanet.com/2021-08/11/c_1127752490.htm.

29. For the first time in the country’s history, the new Five-Year Plan, released on March 13, 2021, does not set a specific GDP target. Instead, it establishes other goals, such as reducing unemployment, increasing life expectancy, lowering carbon-dioxide emissions, and bolstering technological innovation; *see* THE PEOPLE’S GOV’T FUJIAN PROVINCE, OUTLINE OF THE 14TH FIVE-YEAR PLAN (2021-2025) FOR NATIONAL ECONOMIC AND SOCIAL DEVELOPMENT AND VISION 2035 OF THE PEOPLE’S REPUBLIC OF CHINA (Aug. 9, 2021), https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm.

30. *Id.*

31. The Beijing effect, similar to the Brussels effect, indicates the soft power exercised by China at the international level. It consists of a tendency of other countries to imitate and follow the initiatives developed in mainland China. *See generally* Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China’s Digital Silk Road as Transnational Data Governance*, 54 N.Y.U. J. INT’L L. & POL. 1, 1-17 (2021) (arguing that China is exporting its regulatory practice alongside infrastructure investments).

32. *Id.*

economy. The international digital landscape is already altering, given the expansionary influences—epitomized by the Brussels and Beijing effects—and ongoing efforts to decouple domestic infrastructures and technologies supporting data and their circulation. The result is a conflictual dynamic that tugs at the pillars of the shared decentralized, interconnected, and permissionless internet, with the potential to splinter the very foundation of the data-enabled global economy into areas divided by “digital Berlin walls.”³³

As idiosyncrasies solidify, the extraterritorial application of domestic rules reinforces the incompatibility of governance styles. For instance, the *Schrems* cases invalidated the E.U.-U.S. Privacy Shield framework deployed by American companies to comply with the GDPR.³⁴ In a similar vein, the extraterritorial effect of China’s new 2021 Data Security Law in securing sensitive data reflects an even stronger approach to data localization and sovereignty.³⁵ These conflicts are canaries in the coal mine, anticipating much deeper fractures in the global data economy.

Although fragmentation is a ubiquitous phenomenon in international law, the emergence of competing and conflicting non-interoperable data governance regimes and their extraterritorial export result in a “wicked problem.”³⁶ A clear-cut solution is unattainable, since domestic differences and

33. The idea of a “splinternet” foresees reversing the decentralization of internet architecture to allow domestic governments to control and divide traffic around the internet. *See generally* Mark A. Lemley, *The Splinternet*, 70 DUKE L.J. 1397, 1422-27 (2021) (presenting how governments and companies are naturally striving towards controlling the internet); Stacie Hoffmann, Dominique Lazanski & Emily Taylor, *Standardising the Splinternet: How China’s Technical Standards Could Fragment the Internet*, 5 J. CYBER POL’Y 239, 239-47 (2020) (arguing that the splinternet is also a result of diverging technical standards in internet infrastructure, which until now has been generally standardized globally); Kristalina Georgieva, Managing Director, IMF, *From Fragmentation to Cooperation: Boosting Competition and Shared Prosperity* (Dec. 6, 2021) <https://www.imf.org/en/News/Articles/2021/12/06/sp120621-keynote-address-at-the-occd-global-forum-on-competition> (outlining the current trends of technological decoupling and creation of “digital Berlin walls,” with negative impacts for the global GDP).

34. *See* Case C-363/14, *Schrems v. Data Prot. Comm’r*, ECLI:EU:C:2015:650, ¶ 73 (Oct. 6, 2015) (*Schrems I*); Case C-311/18 *Data Prot. Comm’r v. Facebook Ireland Ltd.*, (July 16, 2020) (*Schrems II*); *see generally* Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT’L ECON. L. 771 (2020) (discussing the *Schrems* cases and discussing the consequent possibility of slowing data flows across the transatlantic).

35. *See infra* Section II for a deeper discussion of the Chinese Cybersecurity Law.

36. In general, wicked problems present specific characteristics, such as the lack of a clear understanding of the problem, the impossibility to determine a viable solution, or the inability to test progress against benchmarks. For a discussion of wicked problems in different policy domains, see Udo Pesch & Pieter E. Vermaas, *The Wickedness of Rittel and Webber’s*

conflicting interests render a definitive solution very difficult. As governance styles develop and jurisdictions extend their sovereignty into the digital domain, previously permissionless international data flows become fractured. As data governance styles harden into conflicting, competing, non-interoperable transnational data governance regimes, national interests clash, and international coordination becomes even more difficult. Instead of aiming to work within a global internet-based data system, jurisdictions strive to change its parameters, with material consequences for the global data economy and globalization more broadly. This includes, for example, increasing transaction costs through additional compliance requirements within supply and value chains, or the total breakdown of data transmission that can disconnect commercial, financial, or other markets.³⁷

There is no single solution to the wicked problem of transnational data governance. We identify three possible approaches that could be implemented discretely or in combination to address different critical aspects of the data governance problem. First, in approaching data as a natural resource, we submit that, from a governance standpoint, data presents issues similar to those posed by water (rather than oil), where the lack of an international framework leads to the proliferation of bilateral arrangements (on a case-by-case basis) to resolve jurisdictional conflicts. Building on the riparian practice of water rights management, coordination in transnational data governance could be improved through bilateral arrangements among the three largest

Dilemmas, 52 ADMIN. & SOC'Y 960, 960-72 (2020) (extending the nature of Rittel's wicked problem to institutional setups and broader social changes). In the context of data and technology, commentators have identified different wicked problems. See Jing Zhang & Yushim Kim, *Digital Government and Wicked Problems: Solution or Problem?*, 21 INFO. POLITY 215 (2016) (arguing that digital government has the potential to both empower and disenfranchise citizens); Konstantinos Komaitis, *The 'Wicked Problem' Of Data Localisation*, 2 J. CYBER POL'Y 355 (2017) (noting how localization policies may centralize power, rather than democratizing societies); Linnet Taylor, *Time and Risk: Data Governance as a Super-Wicked Problem* (Feb. 28, 2019) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3344350, (indicating the potentially disruptive outcomes related to the exploitation of data).

37. The international financial system, for example, is utterly dependent on data flows—the decentralized participants of the SWIFT payment messaging system alone accounts for more than 25 billion payments a year. See Boaz B. Goldwater, *Incumbency or Innovation: Why a Collective Agency View of Cross-Border Payments Means Private Blockchains Cannot Prevail Notes*, 52 CORNELL INT'L L.J. 351, 352 (2019–2020) (arguing the unique nature of the international payments system and the role of SWIFT).

economies as well as among others inside or outside their respective data areas. Second, we suggest a regulatory coalition model built on regional or sectoral structures. This approach would build on a shared technological infrastructure, managed by an independent entity, where each jurisdiction decides which channels for data flows are opened and for which purpose. For instance, jurisdictions could maintain existing restrictions on the circulation of personal data, while allowing a free transnational flow of data for trade and financial purposes. Third, we consider a multilateral approach for transnational data governance. This solution could entail the establishment of a new “Digital Bretton Woods” (DBW).³⁸ In particular, a “hard law” framework,³⁹ consisting of treaty-based binding signatory states, would enhance international coordination, establish mechanisms to support data-related negotiations, and drive legal and regulatory harmonization of data governance. However, non-treaty-based “soft law” solutions are more realistic, given the difficulty to achieve an international consensus. In particular, under the aegis of the G20, a non-binding framework might be established.⁴⁰ In this context, a “Digital Stability Board” (DSB) would facilitate international coordination, while supporting the development of harmonized policies, principles, and standards related to data governance.⁴¹ Looking forward, we envisage the most likely

38. The proposal of a Digital Bretton Woods has been animating current policy debate. See Rohinton P. Medhara & Taylor Owen, *A Post-COVID-19 Digital Bretton Woods*, CTR. FOR INT'L GOVERNANCE INNOVATION (Apr. 19, 2020), <https://www.cigionline.org/articles/post-covid-19-digital-bretton-woods/> (noting that a new Digital Bretton Woods model could mitigate the negative implications of the digital revolution); Alex Pentland, Alex Lipton & Thomas Hardjono, *Time for a New, Digital Bretton Woods*, BARRON'S (June 18, 2021), <https://www.barrons.com/articles/new-technologies-will-reshape-the-financial-ecosystem-and-the-world-with-it-51624023107>; Brad Carr, *Digital Services & Data Connectivity: Facing into a Fragmented World*, LINKEDIN (MAR. 27, 2021), <https://www.linkedin.com/pulse/digital-services-data-connectivity-facing-fragmented-world-brad-carr/> (highlighting the absence of a rulebook for the digital global economy and the growing negative consequences).

39. We follow Abbot's and Snidal's definition of “hard law” and “soft law” as non-binary choices along a continuum. Hard law denotes “legally binding obligations that are precise (or can be made precise through adjudication or the issuance of detailed regulations) and that delegate authority of interpreting and implementing the law.” In turn, soft law is when “legal arrangements are weakened along one or more of the dimensions of obligation, precision, and delegation.” See Kenneth W. Abbott & Duncan Snidal, *Hard and Soft Law in International Governance*, 54 INT'L ORG. 421, 421-22 (2000).

40. *Id.*

41. Douglas W. Arner & Michael W. Taylor, *The Global Financial Crisis and the Financial Stability Board: Hardening the Soft Law of International Financial Regulation?*, 32 U. NEW S. WALES L.J., 488, 500-09 (2009) (arguing for the merits of a soft law multilateral regime as a partial substitute for hard law regimes).

result to be a combination of different approaches, extraterritorial, plurilateral, and multilateral, with the best (although not necessarily most likely) case being the creation of a coordinating DSB, along the lines of the G20–initiated Financial Stability Board.

This Article is composed of five parts. Section II outlines the evolving data governance styles and emerging regimes of the United States, China, and the European Union. Section III examines the competing and conflictual dynamics engendered by the emergence of increasingly competitive non-interoperable data governance regimes across the major economies. The analysis focuses on digital sovereignty as the driver for the emerging territorialization of data governance, the expanding role of national security concerns in shaping digital policies, and the splintered character of the global commons that is the internet. Section IV considers the wicked problem of transnational data governance, highlighting three possible approaches: (1) a bilateral approach that draws from the riparian system for water rights; (2) a plurilateral approach allowing the free circulation of data along sector-specific regulatory coalitions; (3) a multilateral approach, either based on a hard law structure, through a new DBW or soft law DSB. Section V concludes by suggesting that the most likely result is a combination of all three approaches. In the best case, coordination at the international level will lead to the establishment of a formal transnational framework; in the worst case, fractures will deepen and the global data economy will splinter into competing, non-interoperable blocs.

II. EVOLUTION OF TRANSNATIONAL DATA GOVERNANCE AND DATA GOVERNANCE STYLES

Over the past thirty years, globalization has been supported by a common approach to data. An extensive cyber regime complex consisting of international organizations, global corporations, non-governmental organizations, and governments alike has underpinned the current permission-less, open, and liberal internet.⁴² The resulting free market for data has enabled

42. The concept of a cyber regime complex was originally introduced by Joseph Nye and has since been expanded. See Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities*, GLOB. COMM'N ON INTERNET GOVERNANCE, No. 1, 7 (May 20, 2014) (arguing for a need to shift analytical focus from a narrow internet governance regime to a broader cyber

data globalization across the global economy, led by large technology and data companies. The dominance of these companies in the new frontier of digital globalization has, not surprisingly, engendered reactions. Starting with the European Union and China, policymakers around the world and now even in the United States have acted to limit the power of such companies. As a result, data has become a focal point of domestic policies, resulting in the intensification of legislative interventions, regulatory initiatives, administrative enforcement actions, and court decisions.

Rather than sporadic attempts to regulate a new area or piecemeal reforms animated by political short-termism, these initiatives take distinct patterns, reflected in domestic data governance styles. Although jurisdictions share the common intent to assert domestic and international control over a strategic policy domain, the idiosyncratic nature of cultural, social, economic, and legal variables, combined with increasingly express strategic competition, generate different emphases on rights, obligations, and accountability mechanisms. Furthermore, the different roles and *modi operandi* of regulatory agencies, courts, and market-discipline mechanisms result in distinct approaches to attain stated policy objectives and interests.⁴³ Drawing from the notion of “regulatory styles,”⁴⁴ we identify emerging data governance styles as the result of several variables observed in each jurisdiction: (1) the general attitude towards markets and this evolving policy domain, as evidenced by the variety of capitalism and governance, policy priorities, and domestic antitrust and competitiveness policy; (2) principles guiding the public interventions in the data economy, as observed by the normative orientation defining the focus of

regime complex with a variety of issue-specific actors). *See infra* Section III.D for a more in-depth discussion.

43. This understanding is reflected in the regulatory governance literature. *See* Black, *supra* note 16. *See also* Karen Yeung, *‘Hypernudge’: Big Data as a Mode of Regulation by Design*, 20 INFO., COMM’N & SOC’Y 118, 120 (2017) (noting that regulatory governance is a process based on three components: gathering information and monitoring; setting standards, goals, or targets; and changing behavior to meet targets).

44. On the notion of regulatory style, see Robert Kagan, *Introduction: Comparing National Styles of Regulation in Japan and the United States*, 22 L. & POL’Y 225, 226-40 (2000) (arguing that there is a difference in regulatory outcome based on the style of regulation in a jurisdiction); R. DANIEL KELEMEN, EUROLEGALISM: THE TRANSFORMATION OF LAW AND REGULATION IN THE EUROPEAN UNION (2011) (depicting differences, similarities and the convergence of US “adversarial legalism” and EU “eurolegalism”); Bignami & Kelemen, *supra* note 17 (defining regulatory styles as a pattern and a *modus operandi* affecting the design and implementation of laws, procedural approaches, adjudication of disputes, and the involvement of courts in the determination of regulatory outcomes).

protections established, and the control attributed to private actors over data; and (3) the regulatory approaches deployed to exercise control through a combination of rule design, and private and public enforcement strategies. Ultimately, a data governance style represents the synthesis of political structures, administrative frameworks, and regulatory approaches. Hence, these styles are not fixed; they evolve, as this Article's analysis of the United States, European Union, and China reveals. As styles evolve, they may harden into regimes, which we argue exists in data governance in the United States, European Union, and China.

By introducing the notion of data governance styles, this Section offers an analytical framework to understand the core dynamics affecting transnational data governance. The evolution of data governance styles in the United States, European Union, and China highlights their emerging differences, which are hardening into competing regimes that differ and conflict. The result is an ever-increasing fragmentation of the paradigm that supported data globalization thus far. This topic will be examined in Section III.

A. TRANSNATIONAL DATA GOVERNANCE AND DATA GOVERNANCE STYLES

Stemming from American approaches towards technology and data embodied on the internet and the foundations of the data economy and data globalization, a libertarian attitude has characterized the framework for transnational data governance since the 1990s, embracing a free market ideology.⁴⁵ This model follows a property-based approach in which all data is alienable. A dearth of government regulation of data movement created a model where data is treated the same as any other commodity and, as such, can be exchanged for value, provided markets are transparent and property rights are protected. This private sector-led approach, combined with the development of open access infrastructure in the form of the internet with limited public sector intrusion beyond funding and support for research and

45. The free market ideology of the internet stems from a "privatization" policy towards many aspects of the internet in the 1990's under the Clinton administration, whereby the U.S. reassigned maintenance of online naming and other infrastructural elements from the initial US defense contractors to the private and non-governmental sector, with minimal regulatory involvement. *See* SCOTT MALCOMSON, *SPLINTERNET: HOW GEOPOLITICS AND COMMERCE ARE FRAGMENTING THE WORLD WIDE WEB* 94–112 (2016).

development and a business-friendly environment, enabled the excesses of the 1990s dot-com bubble while also underpinning globalization.⁴⁶ From these foundations, global access to data has transformed the lives of billions, while enabling Big Tech to rise and dominate the global data commons.

Unlimited data access across jurisdictions through large platforms creates network effects. A consistent stream of new users produces new data, increasing the reliability and the utility of global platforms, thereby attracting more users. In this network-based economy, where data are transferred across jurisdictions and users, network operators acquire exclusive ownership and control over vast pools of data. Hence, the full alienability of data is central to this business model.

By leveraging the knowledge and marketability from data under their control, Big Tech continues to expand across sectors and borders alike. Issues of infrastructural control are also increasingly central to this process. GAFAM and BATs, for example, have built cloud hosting, content delivery, and interconnection platforms that are critical building blocks of the modern internet and digital economy. This architecture of consolidation and control has placed them into the role of content gatekeepers. Control over these elements is only growing, becoming especially critical to ensure the functioning of other IoT and internet reliant structures.

In response, for the past two decades, the European Union has sought to develop a regulatory toolset to curb the influence of private firms and governments over the data of its citizens. Before 2019, China largely followed the U.S. approach to domestic private data (combined with a very different approach to government use of data). Then, the approach shifted, with increasing government control over data flows circulating within China and crossing its borders. Eventually, as China sought to develop its national champions, GAFAM was not allowed within the domestic market. These differences have evolved into divergent and competing data governance styles.

In considering data governance styles, we highlight three sets of variables. The first set of variables pertains to the general attitude that public actors display towards markets and data flows. It describes the inherent cultural

46. See Richard Barbrook & Andy Cameron, *The Californian Ideology*, 6 SCI. AS CULTURE 44, 44-58 (1996) (arguing that the U.S. entrepreneurial class was promulgating a dotcom neoliberalist ideology that found the exploitation of information and knowledge as a utopian driver of growth and wealth).

anchor points characterizing the *why* of data governance in each jurisdiction. This dynamic is assessed through the prism of the political economy framework of “varieties of capitalism,” where data governance measures are layered into strategic interactions of key institutional relationships. Each variety reflects the role of the state and market in the economy, as it emerges from institutional characteristics, political structures, and support to innovation.⁴⁷ The variety of capitalism is a blueprint upon which specific policy priorities are defined to support a public intervention in data governance, such as consumer protection, national security, or market development.⁴⁸ Finally, given the role of competition policies in curbing excessive dominance of data-intensive firms, the general attitude towards markets and data flow is reflected in antitrust law and competitiveness policies.⁴⁹

The second variable refers to the main principles. These principles describe the core normative orientations between the actors, framing the *what* of general legal and non-legal standards of conduct. Principal alignment is characterized by the dialogic focus of a jurisdiction, which can be market, individual, or state-based. Each alignment propels the apportioning of rights and responsibilities that reinforce the primacy of their principles. The ultimate control over data, data agency, and data mobility, for example, differs across jurisdictions to reflect their core principles. As principles are put into regulatory action, they encapsulate an overarching toolbox of legal instruments that further define the regulatory taxonomy of a jurisdiction.

The third variable considers regulatory mechanisms. As emanations of their regulatory systems, regulatory mechanisms denote the proactive and reactive methods for *how* jurisdictions reach policy objectives and ensure adherence to principles. Regulatory mechanisms extend across a continuum between bottom-up, decentralized, and focused on private actors; or top-down, centered, and focused on the public sector. Within this continuum,

47. See generally Beáta Farkas, *Quality of Governance and Varieties of Capitalism in the European Union: Core and Periphery Division?*, 31 POST-COMMUNIST ECONS. 563 (2019) (describing varieties of capitalism and their developmental impact); HALL & SOSKICE, *supra* note 15.

48. BARBARA SCHULTE & MARINA SVENSSON, OF VISIONS AND VISIONARIES: INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) IN CHINA 1-9 (2021) (arguing that ICT realization reflects ideological policy preferences).

49. See FEDERICO ETRO, COMPETITION, INNOVATION, AND ANTITRUST: A THEORY OF MARKET LEADERS AND ITS POLICY IMPLICATIONS 6-26 (2007) (outlining that anti-trust and competition policy is intimately tied to market policy generally).

literature on regulation has identified a range of modes: command-and-control, whereby prescriptive formal measures narrowly describe rights and responsibilities; incentive-based (or market-based), characterized by the offer of financial or other benefits to secure certain behavior; and voluntary compliance, consisting of light regulatory frameworks and self-regulation.⁴⁷ A regulator's place on the continuum is triangulated by linking the design of rules and the approach to their implementation.⁵⁰

The data governance styles of the United States, European Union, and China are converging in establishing data as a strategic priority. Each jurisdiction has set the normative foundations for data governance in higher-level areas including data interoperability, stewardship standards, and sharing.⁵¹ These approaches are increasingly diverging in different policy areas.

B. UNITED STATES: EVOLVING LIBERAL MARKET CAPITALISM

The data governance style of the United States is characterized by liberal market capitalism. Disruption exercised by new business entrants is considered a benefit to innovation and economic growth and is thus fostered.⁵² In line with this tradition, data flows are characterized by free market principles. The internet is, for example, considered a near-libertarian multistakeholder arena where public sector participation is limited to assuring a robust enabling infrastructure.⁵³

50. On the connection of implemented rules and their design, see generally the literature tied to the design of regulatory discretion in public service; MICHAEL LIPSKY, *STREET LEVEL BUREAUCRACY* (1980) (arguing that public service workers in effect are policy decision makers, and thus the design of discretion provided to them is a regulatory choice); Sarah Giest & Nadine Raaphorst, *Unraveling the Hindering Factors of Digital Public Service Delivery at Street-Level: The Case of Electronic Health Records*, 1 *POLY DESIGN & PRAC.* 141 (2018) (arguing that accessibility of digital tools to public service workers is a further choice reflecting broader digital governance decisions); Peter J. May, *Mandate Design and Implementation: Enhancing Implementation Efforts and Shaping Regulatory Styles*, 12 *J. OF POL'Y ANALYSIS & MGMT.* 634 (1993) (arguing that "street-level" implementation of rules is an important aspect of regulatory assessment, as it may differ from codified rules).

51. OECD, *supra* note 13; U.N. Secretary-General, *supra* note 13; Casalini & González, *supra* note 7.

52. See Ingrid Schneider, *Democratic Governance of Digital Platforms and Artificial Intelligence?: Exploring Governance Models of China, the US, the EU and Mexico*, 12 *EJ. OF EDEMOCRACY & OPEN GOV'T* 6-14 (2020) (highlighting the authoritarian, libertarian, and hybrid models of platform governance).

53. See Eric Rosenbach & Shu Min Chong, *Governing Cyberspace: State Control vs. The Multistakeholder Model*, BELFER CTR. FOR SCI. & INT'L AFF. (Aug. 2019), <https://>

The prioritization of a free market is reflected in a dearth of government regulation over data movement. The U.S. data governance style manifests in a regulatory environment that has enabled the GAFAM firms to become Big Tech data market maker platforms that account for more than 55 percent of the used data capacity across the world.⁵⁴ The dynamic also underlies Zuboff's "surveillance capitalism," which argues that a dearth of regulatory oversight in data has resulted in a small concentration of corporate actors wielding substantial power over the social and economic behaviors of consumers around the world.⁵⁵

The light-touch regulation has engendered a minimalist property-based regulatory principle as the anchor point for the United States.⁵⁶ The rights of the government, private, and natural persons are balanced at the locus of agency, which takes place at a contractual level. With narrow exceptions for public and national security, as long as a party is a titleholder to a certain asset, be it real estate, oil, or water—they can alienate this title. Personal or private data rights are thus no different from other property.⁵⁷ Hence, they are completely alienable if stipulated in a consensual agreement.

www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model (presenting different models of internet governance).

54. TELEGEOGRAPHY, THE STATE OF THE NETWORK 3 (2020), <https://www2.telegeography.com/hubfs/assets/Ebooks/state-of-the-network-2020.pdf>.

55. See SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 376-398 (1st ed. 2019) (arguing that the power of nation-states is increasingly dependent on their ability to wield data).

56. The approach has been confirmed by the treatment of data as property in State data privacy laws as well as the trade negotiating objectives of the Trade Promotion Authority legislation. See Illinois Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. 14 (2008) (allowing a cause of action even where no actual injury occurred on the basis of protection of biometric information); California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100-1798.199 (West 2020) (granting individuals the right to request deletion of their personal information); P.L. 114-26, Title I (b)(6)(C) (setting the principal U.S. trade objective in digital trade by "refraining from implementing trade-related measures that impede trade . . . restrict cross-border data flows, or require local storage . . .").

57. There is ongoing discussion on the merits of data as a property right. See Andreas Boerding, Nicolai Culik, Christian Doepke, Thomas Hoeren & Tim Juelicher, *Data Ownership—A Property Rights Approach from a European Perspective*, 11 J. CIV. L. STUD. 323-36 (2018) (drafting the dimensions of how law could establish data as a property right with positive access and negative restriction aspects). See generally P. Bernt Hugenholtz, *Against 'Data Property,'* in KRITIKA: ESSAYS ON INTELLECTUAL PROPERTY 48 (2018) (arguing against data as a property right as it would be restrictive on freedom of information and communication rights); Xiaolan Yu & Yun Zhao, *Dualism in Data Protection: Balancing the Right to Personal Data*

The predominance of the neoclassical laissez-faire approach put forward by the Chicago School of Economics over the past thirty years has shaped the U.S. data economy.⁵⁸ In particular, limited recourse to antitrust law in this field has been a contributing factor to the emergence of Big Tech. Both the Department of Justice and the Federal Trade Commission (FTC) enforce antitrust laws, with the latter also enforcing consumer protection rules. The Sherman Act and Clayton Act are relevant for antitrust enforcement but only saw serious use in the data market in 2019, when the FTC imposed a \$5 billion fine against Facebook for failing to protect user privacy.⁵⁹ The FTC's settlement order also established an independent privacy committee of Facebook's board of directors, removing the CEO's unfettered control of privacy decisions.

The full alienability of data is supported by the adversarial legal system of the United States, as any limitation on contractual freedom is subject to judicial review. Enforcement in the U.S. is legalistic and judges are more likely to reverse administrative decisions curtailing individual rights.⁶⁰ Firms are comparable to political citizens and wield regulatory capacity through the adversarial court system.⁶¹ Though firms generally comply with regulation, they are prepared to disobey in cases of principled disagreement, or where regulation seems arbitrary or unreasonable.⁶² Lawsuits between tech firms testing the boundaries of law are also common with examples like the ongoing *Epic Games v. Apple* and *Epic Games v. Google* cases over preferential cross-platform treatment, or the historic *United States v. Microsoft Corp.* case over browser software bundling.⁶³

and the Data Property Right, 35 COMPUT. L. & SEC. REV. (2019) (arguing that a data property protection system can be created under the Chinese Civil Code).

58. Sandra Marco Colino, *Towards a Global Big Tech Clampdown?*, AGENDA PÚBLICA (2021), <https://agendapublica.elpais.com/noticia/16661/towards-global-big-tech-clampdown> (highlighting a convergence of anti-trust concerns around the world regarding Big Tech data market power).

59. Press Release, Fed. Trade Comm'n, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

60. For this reason, interest groups often resort to court decisions to influence policy outcomes. See Coglianese & Kagan, *supra* note 17 (noting that the adversarial method is among the primary methods of negotiating regulatory change in the United States).

61. Coglianese & Kagan, *supra* note 17.

62. Coglianese & Kagan, *supra* note 17.

63. Friso Bostoën, *Epic v Apple: Antitrust's Latest Big Tech Battle Royale*, 5 EUR. COMP. & REG. L. REV. 79, 79-84 (2021) (describing the implications of the *Epic v. Apple* case for data

The genesis of the dominant philosophy underlying transnational governance of the flow of data, including personal data, stems from the United States, which has historically tacitly embraced the default regulatory doctrine of uninhibited flow of information across borders, with a general prohibition on data localization requirements.⁶⁴ Its negotiation of trade agreements has highlighted its approach to free data flows. The Trans-Pacific Partnership (TPP) as originally drafted and U.S.-Mexico-Canada Agreement (USMCA) regional trade agreements explicitly restrict prohibitions on cross-border transfer of information, forced localization requirements, and forced transfer of source codes.

Because of this adversarial system, proactive regulation is a tool of last resort in the United States, requiring both political will and careful consideration of market impacts. Regulation in the United States features the implementation of detailed provisions that, in an attempt to limit interpretation, increase the level of complexity through prescriptive,⁶⁵ rather than proscriptive, rules. Such prescriptive rules regarding data are rare; they are primarily observed in national security frameworks, such as the CLOUD Act, and the Foreign Intelligence Surveillance Act. Sectoral regulation is light, with examples like the California Consumer Privacy Act or the New York Department of Financial Services Cybersecurity Regulation scattered among states, and efforts at centralization have until recently been nascent.⁶⁶ Instead, data holders generally self-regulate.

companies); Salil K. Mehra, *Data Privacy and Antitrust in Comparative Perspective*, 53 CORNELL INT'L L.J. 133, 134-45 (2020) (outlining U.S. antitrust activity against Big Tech companies).

64. Marcelo Corrales Compagnucci, Timo Minssen, Claudia Seitz & Mateo Aboy, *Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After Schrems II Invalidation of the EU-US Privacy Shield*, 4 EUR. PHARM. L. REV. 153, 154-59 (2020) (finding that SCCs will need to be consistently updated to incorporate necessary information security systems); Thomas Streinz, *The Evolution of European Data Law*, in EVOLUTION OF EU LAW 910-36 (Paul Craig & G. De Búrca eds., 3rd ed. 2021) (noting that E.U. data law gravitates around data protection).

65. Coglianesi & Kagan, *supra* note 17.

66. See John Inglis, *Shining a Light on Cyber*, 14 STRATEGIC STUD. Q. 3, 3-11 (2020) (discussing how cyber-regulation is a growing priority in the United States, but remains underdeveloped as a strategic priority); Jared Bowman, *How the United States is Losing the Fight to Secure Cyberspace* 1-4 (2021) (arguing that the US data governance regime is light in comparison to other major economies); CYBERSPACE SOLARIUM COMMISSION, <https://www.solarium.gov/> 1-19 (last visited Apr 25, 2021) (presenting the need and roadmap for data governance).

In the past decade, this core style has begun to evolve, largely as a reaction to the dominance of GAFAM and (more recently) competition with China. A few landmarks characterize the evolution of the U.S. data governance style and emerging regime. Under the Obama administration, the United States established two paradigmatic policy directions to extend this style. First, the administration escalated cybersecurity to a federal priority through the National Cyber Security Strategy, which has continued under the following administrations.⁶⁷ Second, the administration reinforced the free-trade focus on data by implementing a strict three-prong test for measures that restrict the free flow of information during the negotiation of the TPP.⁶⁸

In 2019, the United States released the Federal Data Strategy. The strategy aims to shift the paradigm in how the government leverages data assets by prioritizing its collection and use and facilitating data for evidence-based policymaking.⁶⁹ The Federal Data Strategy is the culmination of several different legislative and administrative initiatives into a coherent foundational data governance document that moves away from a legacy system for the management of federal data by government agencies. It elaborates upon principles in three categories that aim to reflect and inform agency development and execution through all aspects of the data lifecycle, be they programmatic, statistical, or mission-support oriented. The strategy takes a soft approach, in line with a minimalist property-based paradigm of governing data systems, which balances rights together with commerce and state security interests. Where the European Union's GDPR, for example, requires that one of six legal bases be met for data processing regardless of other processes, under U.S. law, companies can process personal data by default.⁷⁰ The

67. Herb Lin, *How Biden's Cyber Strategy Echoes Trump's*, LAWFARE (Mar. 10, 2021), <https://www.lawfareblog.com/how-bidens-cyber-strategy-echoes-trumps> (discussing how the cyber strategies of the current and previous several terms are similar).

68. Erie & Streinz, *supra* note 31.

69. Russel T. Vought, *Federal Data Strategy - A Framework for Consistency*, OFF. OF MGMT. & BUDGET, <https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf>. See generally O'Hara *supra* note 20 (describing the initial results of the Federal Data Strategy implementation, noting how a trajectory should be set towards creating a national secure data service).

70. Article 6 of GDPR lists the six legal bases as consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

Supreme Court has previously struck state privacy law as being too restrictive of the freedom of speech, confirming its secondary nature.⁷¹ The United States also lacks the dedicated institutional frameworks for data—privacy protection frameworks are piecemeal and sector-specific, while its enforcement is undertaken by the FTC and self-regulation.

The U.S. public sector’s utilization of data is outlined in the Foundations of Evidence-Based Policymaking Act (or OPEN Government Data Act). The act requires that agencies develop evaluation plans linked to their strategic goals and that agencies create learning agendas focused on sequentially asking the “big questions,” and then getting the information necessary to answer them.⁷² The plan must define the data, methods, and analytical approaches used to acquire evidence and facilitate its use in policymaking. Depending on the goals of the agency, strategic evidence-based policymaking should enable them to better understand longer-term societal outcomes and the outputs of their programs. Under the Act, each agency must create an Open Data Plan in which data are cataloged for the public. Within them, data are categorized by tiers of sensitivity, which also decides who has the right to access it. As of yet, the applications for accessing statistical agency data are not centralized and differ between agencies.

Recently, the FTC sued Facebook for illegally maintaining a personal social networking monopoly through anticompetitive conduct.⁷³ The FTC is seeking a permanent injunction that would require divesting the assets of Instagram and WhatsApp—both of which are previous Facebook acquisitions.⁷⁴ Concurrently, the Department of Justice sued Google for maintaining monopolies through exclusionary practices in the search and advertising

free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

71. ZUBOFF, *supra* note 55, at 107.

72. The Act calls for inventorying and publishing all government information as open data. *See* OPEN Government Data Act, S. 2852 114th Cong. (2016). The provisions of the OPEN Government Data Act are now Title H of the Foundations for Evidence-Based Policymaking Act of 2018. H.R. 4174, 115th Cong (2019).

73. *See* Colino, *supra* note 58.

74. Press Release, Fed. Trade Comm’n, FTC Sues Facebook for Illegal Monopolization (Dec. 9, 2020), <https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization>.

markets.⁷⁵ The new approach of the FTC and Justice Department highlights the beginnings of a paradigmatic shift in the U.S. approach to digital competition.

Thus, while the United States can be characterized as following a liberal free-market style, this is evolving, with increasing focuses on decreasing inequality and other tensions, competitiveness, security, and competition.

C. EUROPEAN UNION: COORDINATED MARKET CAPITALISM

The coordinated market capitalism of the European Union extends data governance to the dual priorities of free movement of data within its Single Market and protection of human rights. The removal of legal and technical barriers for the European Union under the four fundamental freedoms of movement for goods, capital, services, and people enables the existence of a Single Market in data. Under a concurrent aegis of human rights, data governance has also aimed to embed a rights-based approach to data reflecting core European cultural values and historical experiences as well as to harmonize and extend consumer protection and data privacy across the twenty-seven Member States.⁷⁶ This framework was a stepping stone for the development of an E.U.-wide data governance style in 1995 with the first Data Protection Directive.⁷⁷ It is this Directive that has been the most commonly adopted framework for data privacy and protection across the world over the subsequent twenty-five years.

At the same time, the European Union did not share the U.S.'s first-mover advantage in technology and data, and its private sector-oriented regulation has evolved to focus on shaping its market and requirements for companies aiming to trade in the European Union. Its “platform gap”—a shortage of market-dominant platforms and the influx of U.S. platforms—has triggered a regulatory response because changes in consumer preferences do not weaken

75. Press Release, Dept. of Just., Justice Department Sues Monopolist Google For Violating Antitrust Laws (Oct. 20, 2020), <https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws>.

76. See Armin Von Bogdandy, *The European Union as a Human Rights Organization? Human Rights and the Core of the European Union*, 37 COMMON MKT. L. REV. 1307, 1309-16 (2000) (arguing that the EU is at its core focused on human rights).

77. Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 431-40 (1994) (highlighting the role of the European Union in pioneering data protection).

the competitive advantage of dominant firms and abuse their power.⁷⁸ The platform gap also restricts the European Union in the development of new information-based technology that is data-heavy and depends on data to create positive feedback loops of better services and better data. Thus, the E.U. approach to data governance in the private sector aims to prevent data concentration and dominance, while also mandating and fragmenting data development for the benefit of new entrants, and concurrently reflects underlying E.U. social and cultural norms towards both the role of data and the role of the private sector. These norms have resulted in the development of an approach based on rights, use, and individual control as opposed to a property rights system, with this embedded in the series of E.U. data protection and privacy rules. Most recently, these norms have culminated in the GDPR for individual ownership and control of data, the Second Payment Services Directive for individual ownership and control of financial data, and the forthcoming data governance and data acts aiming to foster business-to-business and business-to-government data sharing.⁷⁹

These dual priorities are enabled under a rights-based principle. As opposed to the property rights system of the United States, in the European Union, the use of data is constrained by statutory rights that limit the extent to which contractual agreement allows alienation of ownership and control. Though non-personal data are generally alienable, public authorities must retain access to certain data even if located in the other Member States and facilitate data portability procedures between service providers. Personal data, on the other hand, are inalienable from the individual they pertain to because they are considered a protected category. The European Union secures certain rights and control over data use regardless of a potential contractual agreement.⁸⁰

78. A shortage of market dominant platforms and the influx of U.S. platforms has triggered a regulatory response because changes in consumer preferences do not weaken the competitive advantage of dominant firms and abuse their power. See José Van Dijck, *Seeing the Forest for the Trees: Visualizing Platformization and Its Governance*, NEW MEDIA & SOC'Y 2802, 2802-14 (2020) (highlighting the growing complex regimes established around platforms that are causing regulators to aim to reshape the platform system).

79. Streinz, *supra* note 64 (presenting an overview of the burgeoning E.U. data governance framework).

80. Interesting parallels can be drawn between the regime enacted by several E.U. jurisdictions regarding inalienable intellectual property licenses. See Andrea Tosato, *Secured*

In 2018, the European Union adopted regulations on the mobility of non-personal data.⁸¹ In this framework, non-personal data can circulate freely within the Single Market; personal data, however, are subject to much stricter GDPR rules.⁸² The GDPR allows the export of personal data only in compliance with the extraterritorial application of local data privacy rules. In particular, if personal data are processed overseas, the receiving jurisdiction must ensure that domestic rules meet adequacy requirements, whereby the transborder flow of personal data outside the Single Market can only occur if a certain level of protection is ensured.⁸³ When a jurisdiction meets such requirements and the European Commission grants the adequacy recognition, data can circulate freely between the Single Market and the third jurisdiction. The adequacy rules have been tested for their limits—Google resisted French requests to universally delist search results based on the E.U. right to be forgotten in *Google Inc. v. Commission nationale de l'informatique et des libertés*, limiting the result of adequacy decisions to within E.U. borders.⁸⁴ The GDPR also allows Member States to enact additional limits on the free circulation of personal data. Member States can, for example, enact data localization measures, in the context of health, financial services, or other sectors.⁸⁵

The European Union's rights-based data approach was established by adopting a series of statutory instruments. GDPR structures consent-based data relationships between data subjects, controllers, and handlers, providing

Transactions and IP Licenses: Comparative Observations and Reform Suggestions, 81 L. & CONTEMP. PROBS. 155, 161-163 (2018).

81. Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, 2018 O.J. (L 303) 59.

82. Streinz, *supra* note 64.

83. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

84. In this case, the Court of Justice held that there is no obligation for Google to apply the European right to be forgotten globally, limiting the territorial withdrawal of information within the European Union. *See* Case C-507/17, *Google v. CNIL*, EU:C:2019:772 (Sept. 24, 2019).

85. Nigel Cory, Robert D. Atkinson and Daniel Castro, *Principles and Policies for "Data Free Flow With Trust"*, INFO. TECH. & INNOVATION FOUND. (May 27, 2019), <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust/> (highlighting the limits of data protection under the GDPR); Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, INFO. TECH. & INNOVATION FOUND. (May 1, 2017), <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/> (highlighting the transaction costs of data protection regimes).

subjects the right to be forgotten and personal data transfers at request.⁸⁶ The eIDAS regulation, for example, builds on this consent basis to establish an E.U.-wide digital ID regime for digital access to cross-border public and private services.⁸⁷ In turn, non-personal data are regulated under the Regulation framework for the free flow of non-personal data in the European Union, requiring frictionless movement of data across E.U. Member States. A series of forthcoming laws aim to further expand on the rules for domain-specific data spaces, public-private data sharing,⁸⁸ and the data duties of large gatekeeper platforms.⁸⁹

The European Union also actively pursued competition cases as a reflection of its concerns over dominance and control of data and technology. Between 2017 and 2019, the European Commission fined Google three times for abusing its dominant position.⁹⁰ Germany's Federal Supreme Court upheld a 2019 decision against Facebook, confirming that the latter abused its dominant position in the German market, requiring Facebook to stop collecting data about its users without their consent.⁹¹ The suite of rules,

86. See Max von Grafenstein, Alina Wenick & Christopher Olk, *Data Governance: Enhancing Innovation and Protecting Against Its Risks*, 54 INTERECONOMICS 228, 228-32 (2019) (presenting the need to reduce the risks of rampant data-based innovation).

87. These efforts aim to support the recently established E.U. 2030 digital targets, undertaking the digitization of key public services, e-health, and identity. *Europe's Digital Decade: Digital Targets for 2030*, EUR. COMM'N, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (last visited Mar. 26, 2021).

88. This occurs in the context of domain-specific initiatives, as it is the case of the Second Payments Services Directive. Broader, cross-sectoral initiatives include the Data Governance and upcoming Data Acts that, inter alia, aim to foster business-to-business and business-to-government data sharing on different areas. See Ginevra Bruzzone & Koenraad Debackere, *As Open as Possible, as Closed as Needed: Challenges of the EU Strategy for Data*, 56 LES NOUVELLES-J. LICENSING EXECS. SOC'Y 41, 41-48 (2021) (offering an analysis and outlining the weaknesses of current data sharing initiatives in the E.U.).

89. For instance, the upcoming Digital Markets and Services Acts aim to prevent anti-competitive behavior from large gatekeeper platforms, see *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data* COM (2020) 66 final (Feb. 19, 2020).

90. See generally Christophe Carugati, *Competition Law and Economics of Big Data: A New Competition Rulebook* (Nov. 16, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717420 (addressing competition law issues for Big Tech).

91. Klaus Wiedemann, *A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19)*, 51 INT'L REV. INTELL. PROP. & COMPETITION L. 1168, 1174-80 (2020) (highlighting the ways

together with an active pursuit against anti-competitive practices places data companies aiming to compete under the E.U. framework into a share-by-design data market, where the growth of data concentration is significantly halted.

The E.U. approach to digital competition entails preventative measures under the precautionary principle.⁹² A suite of regulations aims to create an environment that fosters the development of competitive data enterprise in the E.U. market while preventing the further concentration of GAFAM and Chinese competitors operating in Europe.⁹³ Beyond establishing the rights of individuals to control their personal data, the European Union set out several legislative initiatives to avert the singular aggregation of data-based market power.⁹⁴ These priorities also underpin the emerging E.U. aim to secure control over data produced in its territory under the concept of “digital sovereignty.”⁹⁵ In 2020, the European Union announced a paradigmatic policy shift via novel strategies for data, by creating domain-specific “data spaces” that aggregate data within and across different sectors, with unique infrastructures, rules, data-sharing tools, platforms, and data interoperability for each.⁹⁶ Through such policies, the European Commission aims to close the “platform gap.” The 2020 Platform to Business Regulation requires online platforms and search engines to provide clear and transparent terms and conditions regarding parameters for determining ranking and differentiated treatment.⁹⁷ The proposal for the Data Governance Act sets out the rules for

in which EU Member States can enact stronger data protection rules nationally than required by EU rules).

92. Aurelien Portuese, *Precautionary Antitrust: A Precautionary Tale in European Competition Policy*, in L. & ECON. REGUL. 203 (2021) (presenting the use of new regulatory and technological tools in the European Union antitrust regime as an example of a preference towards precaution over innovation and disruption).

93. Rocco Bellanova, Helena Carrapico & Denis Duez, *Digital/Sovereignty and European Security Integration: An Introduction*, 31 EUR. SEC. 337 (2022) (arguing that the inhibiting impacts of GAFAM on innovation and economic development have led to a more interventionist regulatory stance in the European Union).

94. *Id.*

95. Ursula von der Leyen, State of the Union Address by President von Der Leyen at the European Parliament Plenary (Sept. 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655.

96. *Id.*

97. *Platform-to-Business Trading Practices - Shaping Europe's Digital Future*, EUR. COMM'N, <https://digital-strategy.ec.europa.eu/en/policies/platform-business-trading-practices> (last visited June 23, 2021).

sharing data among businesses and foresees the creation of neutral data intermediaries that can act as trusts for this data.⁹⁸ Lastly, the Digital Markets Act establishes a criterion for qualifying large online platforms as “gatekeepers,” which must permit third parties to interoperate within their ecosystems, allow business users to access data generated through the use of the platform, and prevent the treatment of self-services and products more favorably than those of third parties.⁹⁹

At the core of the E.U. public-sector strategy is the cross-sectoral removal of legal and technical barriers to data sharing across organizations through the creation of domain-specific “data spaces” with unique infrastructures, rules, data-sharing tools, platforms, and data interoperability.¹⁰⁰ The European Commission posits these harmonized data-driven cloud-based ecosystems as the key to unlocking European “data pools,” which enable benefits from big data analytics and machine learning. The approach to each data space will be unique, unified by principles of findability, accessibility, interoperability, and reusability.¹⁰¹

To operationalize the vision for its data governance strategy, the European Commission aims to create a single cross-sectoral governance framework for data access and use. Data will be made available for re-use for public and private sector participants through machine-readable formats and Application Programming Interfaces (APIs). The Commission will set additional horizontal and vertical data sharing requirements between public and private sectors through the forthcoming Data Act.¹⁰² It will assess necessary measures

98. *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, COM (2020) 767 final (Nov. 25, 2020).

99. Luis Cabral, Justus Haucap, Geoffrey Parker, Georgios Petropoulos, Tommaso Valletti & Marshall Van Alstyne, *The EU Digital Markets Act: A Report from a Panel of Economic Experts*, EUR. COMM’N JOINT RSCH. CTR. (2021).

100. For a description of data spaces in the European Union, see generally *Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, COM (2022) 68 final (Feb. 24, 2022), <https://op.europa.eu/en/publication-detail/-/publication/d0f2ed7a-9664-11ec-b4e4-01aa75ed71a1/language-en> (outlining the positive impacts of a data governance act on the European Union, finding that such regulation is necessary to ensure that more public and private actors benefit from Big Data and machine learning techniques).

101. *Id.*

102. *Id.*

for the establishment of specific data pools for machine learning and data analysis. Nine data spaces are initially planned, with more under consideration: industrial, Green Deal, mobility, health, financial, energy data, agriculture, public administration, and skills data.¹⁰³ These data spaces will feed into the recently established 2030 digital targets, which are aimed at the total digitization of key public services, e-health, and identity. The 2019 revision of the public sector information directive also requires that non-personal data held by public bodies be open for commercial and non-commercial reuse free of charge.¹⁰⁴

These regulatory bundles mix outcome-based rules with enforced self-regulation for personal and non-personal data, respectively. The outcome-based regulation is enforced through institutional networks and entrusting E.U. courts to challenge and legitimize regulation.¹⁰⁵ The Court of Justice of the European Union (CJEU) and the European Court of Human Rights have, for example, repeatedly upheld fundamental privacy and consumer protection rights.¹⁰⁶ The European Commission has also fined Google for abuse of its dominant position in digital-advertising and comparison-shopping markets.¹⁰⁷ However, non-personal data are generally self-regulated in the European

103. *Id.*

104. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), 2019 O.J. (L 172) 56.

105. Chase Foster, *Legalism Without Adversarialism: Public and Private Enforcement in the European Union* 10-14 (June 2020) (working paper), https://www.chasefoster.com/_files/ugd/892c68_f9222e3d55d44d59ae020f39b64cbe4a.pdf (arguing that E.U. legislation does not encourage the private enforcement of public law, but courts still play an important role in legitimizing rules); Lincey Bastings, Ellen Mastenbroek & Esther Versluis, *The Other Face of Eurolegalism: The Multifaceted Convergence of National Enforcement Styles*, 11 REG. & GOVERNANCE 299, 304-11 (2017) (highlighting that there is a level of adversarialism present in the E.U. legal system).

106. Enumerated in Charter of Fundamental rights and European Convention on Human Rights. See OLIVER PATEL & NATHAN LEA, EU-U.S. PRIVACY SHIELD, BREXIT AND THE FUTURE OF TRANSATLANTIC DATA FLOWS 9 (2020) (highlighting human rights as a basis for the breakdown of the Privacy Shield regime).

107. For example, in 2019 the European Commission fined Google for abusing its data in online advertising. See Press Release, Eur. Comm'n, Antitrust: Google Fined €1.49 Billion for Online Advertising Abuse (Mar. 20, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770

Union, with statutes creating a variety of “self-regulatory codes” for issues like data portability, or risk-based systems to prevent abuse of users.¹⁰⁸

D. CHINA: FROM ORGANIZED TO CONTROLLED CAPITALISM?

China’s evolving data governance style emerges from the primacy of the twin objectives of (1) stability (social, financial, economic, and national security) and (2) innovation, development, and competitiveness through a matrix of interlocking command-and-control regulations.¹⁰⁹ These goals manifest in a closely intertwined public and private sector relationship, where data in the domestic market before 2020 was largely treated similarly to data in the United States in the context of private markets, with full alienability and resulting in similar dynamics to those seen in the United States: the evolution of a small number of large dominant data firms.¹¹⁰ At the same time, particularly over the past decade, the domestic market was largely protected from foreign competition (particularly from the United States). In parallel, from the standpoint of public sector data access and use, China is unique both in attitudes supporting such access and in the technical mechanisms and ability of the central government to access data for public policy interests. This nexus enables a vast digital autarky over what amounts to almost a third of global data flows.¹¹¹

The Chinese data market is characterized by a combination of a property-based approach similar to that of the United States in the context of private-sector acquisition and control of data, combined with restriction of external competition in the form of import substitution and close cooperation with the state for broader governmental objectives. In China, the state works closely with the non-state sector. China blocks access to ten of the top twenty-five top global websites to support the evolution of a “parallel universe” of

108. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018 O.J. (L 303) 59.

109. See Rogier Creemers, *China’s Conception of Cyber Sovereignty*, in DIGIT. TECHS. & GLOBAL POL. DIPL. 107, 107-15 (Dennis Broeders & Bibi van den Berg eds., 2020) (discussing the overarching goals of Chinese data governance policy).

110. *Id.*

111. Aho and Duffield, *supra* note 21; Wei Yin, *A comparison of the US and EU regulatory responses to China’s state capitalism: implication, issue and direction*, 19 ASIA EUR. J. 1, 1–25 (2021) (discussing the size of China’s state-centric form of capitalism).

domestically dominant Chinese platforms (e.g., Alibaba, Weibo, Baidu, and QQ).¹¹² The flexibility of skipping domestic development of desktop computing allowed China to leap toward innovation in mobile computing, enabling rapid adoption of new approaches.¹¹³

Both policy priorities are central to China's concept of "cyber sovereignty." Cyber sovereignty positions the digital environment and internet as areas for sovereigns to exercise their sovereign rights against other actors domestically and internationally. Through this lens, China enacts a high level of centralized control over data to protect national security interests, but also to guarantee its ability to intervene in the development of the domestic market.¹¹⁴ Since 2017, China has taken an increasingly state-centered approach to cyber sovereignty, reflected in its development of a comprehensive regulatory governance framework. Three laws are the pillars of this approach: the 2017 Cybersecurity Law,¹¹⁵ the 2021 Data Security Law, and the 2021 PIPL.¹¹⁶ Based on these rules, China has also strived to limit private company dominance of data by bringing a series of regulatory actions against Ant, Tencent, Didi, and others.¹¹⁷ The combination reflects an evolution in governance style that moves from a pro-private sector and innovation approach, albeit with state guidance, support, and involvement, to one much more expressly centered on the twin state objectives of stability and development.

Both priorities emanate from a state-centric normative orientation to the evolving framework, as reflected in a new state council policy framework in

112. Sebastian Hermes, Eric Clemons, Maximilian Schreieck, Simon Pfab, Maya Mitre, Markus Bohm, Manuel Wiesche & Helmu Krcmar, *Breeding Grounds of Digital Platforms: Exploring the Sources of American Platform Domination, China's Platform Self-Sufficiency, and Europe's Platform Gap*, EUR. CONF. ON INFO. SYS. JUNE 2020, https://aisel.aisnet.org/ecis2020_rp/132/ (discussing the access dynamic between online platforms around the world).

113. *Id.*

114. SCHULTE & SVENSSON, *supra* note 48.

115. PRC Cybersecurity Law, *supra* note 26.

116. PRC Data Security Law, *supra* note 27; PRC Personal Information Protection Law, *supra* note 27.

117. China's tech crackdown saw record-large fines against the country's largest tech companies in fintech, ecommerce, ride hailing, social media, insurance, and other sectors. Many of these fines were related to the mishandling of consumer data, and anti-competitive practices. In the case of certain tech firms like Didi, the company was required to delist from the New York Stock Exchange and move to Hong Kong. For more, see *China's Big Tech Crackdown: A Complete Timeline*, THE CHINA PROJECT, <https://thechinaproject.com/big-tech-crackdown-timeline/> (last visited Jan. 14, 2023).

August 2021.¹¹⁸ While control over data under the emerging system follows the hybrid model of the European Union, attaching inalienable rights to personal data while allowing higher levels of alienability to non-personal data, ultimate control over data belongs to the central government. Not only does the government have access to data, but it also mandates data collection and analysis in both the public and private sectors. Though the government allows uninhibited flows internally, data can only leave or enter China with express government permission.¹¹⁹

China practices an increasingly restrictive stance on data mobility, as stipulated in the Data Security Law and the PIPL.¹²⁰ Any personal information generated within China must be stored within the physical jurisdictional territory, and any data export is under the centralized discretion of the Chinese data regulator, the Cyberspace Administration of China.¹²¹ Concurrently, any processing of personal information outside of the Chinese jurisdiction requires that the processor retains representation in China.¹²²

The state-centric principle is implemented through rule-based regulation. A sprawling framework of regulation under the umbrella priority of cyber-sovereignty sets data flows as a critical matter of national security, with corresponding duties for digital stakeholders. The Data Security Law establishes tiers of protected data, starting with “core state data” that includes issues of national security, national economy, or aspects of people’s livelihoods that must undergo stringent cybersecurity approval procedures.¹²³ The

118. PRC Cybersecurity Law, *supra* note 26; PRC Data Security Law, *supra* note 27; PRC Personal Information Protection Law, *supra* note 27; XINHUA NEWS AGENCY, *supra* note 28.

119. Angela Huyue Zhang, *Agility Over Stability: China’s Great Reversal in Regulating the Platform Economy*, HARV. INT’L L.J. 26-40 (forthcoming 2022) (highlighting China’s expanding regulatory oversight via antitrust, financial, and data regulation); Hermes et al., *supra* note 112.

120. For example, Article 25 of the Data Security Law stipulates the establishment of a “export controls” on data for national security interests. *See* PRC Data Security Law, *supra* note 27.

121. Article 38 of the PIPL stipulates that personal information can only be provided outside of China with approval or a security assessment by state institutions. *See* PRC Personal Information Protection Law, *supra* note 27.

122. *See* PRC Personal Information Protection Law, *supra* note 27 at art. 39.

123. PRC Data Security Law, *supra* note 27. *See*, in particular, rules related to national security, the lifeline of the national economy, important aspects of people’s livelihoods under Chapters II, III, and IV.

Cybersecurity Law requires, for example, all “network operators”¹²⁴ that own, manage, or provide network services, to monitor and supervise the behavior of its users and “assist” in government requests.¹²⁵ While the PIPL establishes rules for personal data handling based on explicit consent, requiring short data retention time or allowing requests for deletion of personal data, it also provides for express circumventions if other laws, like the Cybersecurity Law, require such information.¹²⁶

Rules are enforced under a command-and-control praxis. One manifestation of this mode is in statutes. Refusal to provide assistance to relevant departments makes network providers criminally liable under the Cybersecurity Law.¹²⁷ The Data Security Law, also expresses that the results of security reviews are “final.” Another manifestation is through the “pervasive threat” of discretionary use of administrative tools by government agencies that can provide benefits or cause detriments to businesses, such as through rationing resources, licenses, or creating informal burdens.¹²⁸

The Chinese regulatory approach to digital competitiveness manifests in “digital mercantilism” focused on securing economic stability.¹²⁹ The 2015 “Made in China 2025” strategy issued by the Chinese State Council expressly aims to support the integration of information technology and industry and promote breakthroughs in key information technology sectors.¹³⁰ Many of these strategies expressly depend on the mobilization of state-owned enterprises, the preferential allotment of capital to domestic companies, and the forced transfer agreement requiring foreign companies to transfer

124. Operators of critical information infrastructure are an additional separate category of subjects, dealing largely with state activities. *See* PRC Data Security Law, *supra* note 27 at art. 31.

125. *See* PRC Cybersecurity Law, *supra* note 26.

126. *See* PRC Data Security Law, *supra* note 27; PRC Personal Information Protection Law, *supra* note 27.

127. *See* PRC Cybersecurity Law, *supra* note 26.

128. *See* Xiaofan Zhao & Ye Qi, *Why Do Firms Obey?: The State of Regulatory Compliance Research in China*, 25 J. CHIN. POL. SCI. 339, 346-49 (2020) (highlighting informal methods of ensuring compliance in China).

129. *See* C.Y. Cyrus Chu & Po-Ching Lee, *E-Commerce Mercantilism-Practices and Causes*, J. INT'L TRADE L. & POL'Y 51, 53-59 (2020) (outlining a practice of digital mercantilism through asymmetrical internet access in China).

130. 2025 zhōngguózhìzào èr líng èr wǔ (中国制造) *Made in China 2025*, promulgated by the State Council on July 7, 2015, <https://perma.cc/9PA3-WYBA>, *translated in* CTR. FOR SEC. & EMERGING TECH. (Mar. 8, 2022), https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf.

intellectual property through forced joint ventures with local competitors.¹³¹ Though China has committed to regulating against the forced transfer of technology by foreign firms, via the U.S.-China Trade Agreement of January 15, 2020, and the E.U.-China Comprehensive Agreement on Investment, forced IP handovers have not yet been addressed by regulatory measures in China. This has consequently resulted in a WTO dispute initiated by the United States.¹³²

The quasi-public sector character of major tech platforms in China also adds an additional layer of complexity to regulating digital competition. Recently, the People's Bank of China, the country's central bank, together with other regulatory agencies ordered 13 of the largest technology firms to unbundle and restructure the internet-based businesses' financial businesses into licensed financial service providers.¹³³ With this move, the Chinese authorities can bring digital financial activities within the regulatory perimeter of financial regulation to "break [the] information monopoly" and "enhance the sense of social responsibility."¹³⁴ However, the explicit delegation of pseudo-public functions to major platforms (like the right of Alibaba to legally prosecute individuals and businesses breaching rules on its platform, or the total access of the Chinese government to company data) skews competition interests towards ensuring a thriving, yet protectionist internal market.¹³⁵ Though foreign internet users can access Chinese websites, those aiming to

131. For a discussion on China's state support to its private sector, see generally USHA C. V. HALEY & GEORGE T. HALEY, *SUBSIDIES TO CHINESE INDUSTRY: STATE CAPITALISM, BUSINESS STRATEGY, AND TRADE POLICY* (2013) (highlighting a trend in China to support local companies).

132. Paolo Beconcini, *International Challenges Help China and the EU Find Agreement on Technology Transfer*, NAT'L L. REV. (Jan. 14, 2021), <https://www.natlawreview.com/article/international-challenges-help-china-and-eu-find-agreement-technology-transfer>.

133. See Keith Zhai, *China Orders Tech Giants to Unbundle Financial Services*, WALL ST. J. (Apr. 30, 2021), <http://www.wsj.com/articles/china-orders-tech-giants-to-unbundle-financial-services-11619780759>. (the 13 firms include Tencent, Du Xiaoman Financial, JD Finance, ByteDance, Meituan Finance, DiDi Finance, Lufax, Airstar Digital Technology, 360 DigiTech, Sina Finance, Suning Finance, Gome Finance, and Ctrip Finance).

134. *Id.*

135. Lizhi Liu, *The Rise of Data Politics: Digital China and the World*, 56 STUD. COMP. INT'L DEV. 45, 46-54 (2021) (outlining concerted governance efforts to protect burgeoning digital markets); Lizhi Liu & Barry R. Weingast, *Taobao, Federalism, and the Emergence of Law, Chinese Style*, 102 MINN. L. REV. 1563, 1573-87 (2017) (highlighting a unique form of delegating administrative governance functions to digital platforms).

enter the Chinese market have little choice but to use Chinese platforms like Weibo. In part because of these mercantile and protectionist policies, in 2018 China accounted for 40 percent of the total revenue of the top ten digital trade operating countries.¹³⁶ Looking forward, these data capacities are being embedded and reinforced through a sophisticated Social Credit System that makes use of a centralized digital ID program and an experimental Digital Yuan initiative to interlink individuals, businesses, and social organizations.¹³⁷

The variables characterizing each domestic style are consolidating into increasingly contrasting and, in many cases, conflicting data governance regimes. The result is a reversal of the data globalization process and a growing fragmentation of data flows and infrastructure. In fact, the findings of the style analysis (summarized in Table 1) indicate that the three major economies pursue uncooperative strategies to address shared policy concerns over national security, international competitiveness, and control over private actors. Furthermore, they adopt substantially different approaches to regulated ownership and control of data, emphasizing: property entitlements to support a market-based economy for data (the United States); consumers' rights to protect end-users (the European Union); and State centralization to pursue broader social and economic policies (China). Finally, from a practical standpoint, the mode in which domestic regulatory rules are designed and enforced differs substantially, with different reliance on the cooperation of regulated entities to implement regulatory regimes.

136. See Chu & Lee, *supra* note 129.

137. Jacqueline Hicks, *Digital ID Capitalism: How Emerging Economies are Re-inventing Digital Capitalism*, 26 CONTEMP. POL. 330, 330-50 (2020) (advancing an emerging digital ID-centric market).

Table 1. Governance Styles of the US, EU, and China: Key Variables

	Market Attitude			Guiding Principles			Regulatory Approaches	
	<i>Variety of capitalism</i>	<i>Policy priorities</i>	<i>Antitrust and competitiveness</i>	<i>Normative orientation</i>	<i>Personal data control/mobility</i>	<i>Non-Personal Data control/mobility</i>	<i>Mode of Regulation</i>	<i>Mode of Enforcement</i>
US	Liberal	Free market National security	Market efficiency	Property-based	Individual control established on contractual basis (with full alienability) Free data flow	Individual control established on contractual basis (with full alienability) Free data flow	Adversarial	Self-regulation
EU	Coordinated	Single Market creation and protection	Consumer-focused	Rights-based	Individual control (with non-alienable data) Restricted data flow	Individual control established on contractual basis (with full alienability) Free data flow	Outcome-based regulation	Enforced-self regulation
China	Organized	Cybersecurity Internal market development	Economic stability	State-based	State control (with non-alienable data) Restricted data flow	State control (with non-alienable data) Restricted data flow	Rule-based regulation	Command-and-Control

The consolidation of data governance styles and the emergence of competing and even conflicting data governance regimes has resulted in a fragmented transnational data governance framework. The consequences of this process are most clearly seen in the context of the global commons—a framework of institutional arrangements for the governance of globally shared resources among its stakeholders.¹³⁸ The internet, run on open source, non-exclusive and non-proprietary protocols is one such emergent global commons.¹³⁹

138. Jennifer Shkabaturo, *The Global Commons of Data*, 22 STAN. TECH. L. REV. 354 (2019) 383 (discussing how the data, utilizing the underpinning internet infrastructure, should be considered a global commons from a relational perspective).

139. *Id.*

III. FRAGMENTATION OF TRANSNATIONAL DATA GOVERNANCE: SOVEREIGNTY, COMPETITION, AND SECURITIZATION

Distinct data governance styles are evolving, which reflect different attitudes towards markets, policy priorities, principles, and regulatory approaches. Crucially, reactions to Big Tech's dominance have prompted initiatives to assert sovereignty over the digital world—first, in the European Union, then in China, and eventually in the United States. Over the past decade, concerns about data security have refocused on security (both individual and national) and competitiveness issues, as societies look to maximize the benefits of data for their own development while controlling risks of digitalization. The result is an international landscape where the three major economies compete to gain control and expand their influence over data and data flows.

Tensions and conflicting positions have become increasingly more apparent, besetting the process of data globalization that started three decades ago. The fracturing of the internet is the likely eventual result, as data can flow freely only within jurisdictional areas meeting potentially non-interoperable idiosyncratic requirements. At the global level, a new form of digital competition among major actors is emerging and is buttressed by the pursuit of digital (or data) sovereignty. To gain control, jurisdictions harden their stances, by exercising extraterritorial application of their laws, and by tightening access to and circulation of data for national security purposes.

This Section examines these dynamics, beginning with digital sovereignty as an emerging central priority. The process of data securitization highlights how the expansion of national security and defense policies is halting the process of data globalization. This can be seen most directly in the context of the impact on the internet, by identifying how conflicts beset the global data infrastructure.

A. DIGITAL SOVEREIGNTY

Digital sovereignty is an emerging concept with blurred contours.¹⁴⁰ Broadly, it refers to the level of control over data, infrastructure, and standards

140. On the different connotation of “digital sovereignty”—also referred to as “data sovereignty” or “cyber sovereignty”—see Patrik Hummel, Matthias Braun, Max Tretter & Peter Dabrock, *Data Sovereignty: A Review*, 8 BIG DATA & SOC'Y 1, 9-12 (2021) (providing a

held by a State vis-à-vis other States, private firms, and individual citizens.¹⁴¹ It manifests as regulatory, legal, or technical control that state actors and private actors exercise, among and between them, over the digital world.¹⁴²

Digital sovereignty also enables competition between data governance regimes. In fact, each jurisdiction seeks to expand its influence internally and externally by devising regulatory and technological solutions that can be adopted across the world. This phenomenon extends beyond traditional explanations for regulatory competition between jurisdictions. In the literature, it is often noted that market participants may choose to operate in different legal systems to maximize their revenues, thus spurring regulatory competition.¹⁴³ Studies have shown that this competition can have virtuous effects, pushing policymakers to devise more efficient rules in a race to the top where jurisdictions compete to design increasingly better rules, a phenomenon known as the “California effect.”¹⁴⁴ Yet, negative consequences may surface

systematic review of data sovereignty studies, and highlighting the most common associations being with control and power, security, representation, and privacy); Luciano Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 PHIL. & TECH. 369, 371 (2020) <https://doi.org/10.1007/s13347-020-00423-6>.

141. Alexandru Circumaru, *The EU’s Digital Sovereignty—The Role of Artificial Intelligence and Competition Policy 1-10* (2021) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3831815 (describing the three main characteristics of EU digital sovereignty as “autonomy, ability to influence, and protection of EU citizens’ self-determination online”).

142. Creemers, *supra* note 109 (proposing four dimensions to assess digital sovereignty in any given jurisdiction: (i) the target of sovereignty and at whom the claim of sovereignty is aimed, (ii) the nature of the sovereignty claim in regard to the specific legal entitlements it constitutes, (iii) the objectives of the pursuit of sovereignty, and (iv) the means to realize sovereignty through legal-regulatory tools).

143. The concept of regulatory competition has been extensively examined since the 1950s, with the original analytical framework offered owed to Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416 (1956). Different models have been developed to explain regulatory rivalry and competitive dynamics within federal, supranational, or international markets for legal rules; see Claudio M. Radaelli, *The Puzzle of Regulatory Competition*, 24 J. PUB. POL’Y 23 (2004) (offering an overview and a critique of traditional models explaining regulatory competition).

144. Richard Perkins & Eric Neumayer, *Does the ‘California Effect’ Operate across Borders? Trading and Investing-up in Automobile Emission Standards*, 19 J. EUR. PUB. POL’Y 217, 217-25 (2012) (using the example of automobile emission standards to find developing country automobile exports to countries with more stringent standards as a cause for more stringent standards in the exporting country); Dirk A. Heyen, *Influence of the EU Chemicals Regulation on the US Policy Reform Debate: Is a ‘California Effect’ within REACH?*, 2 TRANSNAT’L ENV’T L. 95,

when rules are relaxed to attract more market participants, thus, spurring a race to the bottom, also known as the “Delaware effect.”¹⁴⁵ In the context of data governance, the competition between governance regimes cannot, at least in its current form, be encapsulated in this traditional dynamic. Domestic policymakers are concerned with expanding their sovereignty in the digital world vis-à-vis state and private actors alike.

Over the past several decades, the dominant liberal market approach to data and the internet has underpinned the evolution of the global data economy. Together with the first-mover advantage impetus reflected in the motto “move fast and break things,”¹⁴⁶ the American style of data governance became a model for most jurisdictions aiming at establishing a domestic Silicon Valley. As policymakers of different jurisdictions adopted a laissez-faire attitude towards data flows and data-intensive firms, the resulting process of data globalization reinforced the dominance of Big Tech. As the European Union began to set its own minimum rules for data governance in its internal market, it began to trigger the Brussels effect—as foreign companies trading in the Single Market had to adjust their conduct to fit the European Union’s standards, the same companies are incentivized to lobby the standardization of such rules in their domicile nation-states.¹⁴⁷ While this was largely voluntary under the pre-GDPR approach of the 1995 Data Protection Directive (and widely adopted arguably as a reflection of the California effect of the attraction of the E.U. approach as an alternative to that of the United States), GDPR’s data transfer rules are increasingly forcing the adoption of similar approaches

95-110 (2013) (finding the California effect from stringent E.U. chemicals standards to exported countries, but not to large trading partners like the United States).

145. The California and Delaware effects are two sides of the same conceptual coin and have been broadly discussed. See DAVID VOGEL, *TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY* 1-40 (2009) (introducing the concept of the California effect in an environmental rules contexts); Richard Perkins & Eric Neumayer, *Does the ‘California Effect’ Operate across Borders? Trading-and Investing-up in Automobile Emission Standards*, 19 J. EUR. PUB. POLY 217, 217-28 (2012) (presenting the trans-jurisdictional evidence of the California effect); Fernán Restrepo & Guhan Subramanian, *The Effect of Delaware Doctrine on Freezeout Structure & Outcomes: Evidence on the Unified Approach*, 5 HARV. BUS. L. REV. 205, 205-17 (2015) (discussing the Delaware effect in the context of buyouts).

146. Until recently, this was the internal motto of Facebook, according to its founder. See Drake Baer, *Mark Zuckerberg Explains Why Facebook Doesn’t “Move Fast And Break Things” Anymore*, BUS. INSIDER, (May 2, 2014) <https://www.businessinsider.com/mark-zuckerberg-on-facebooks-new-motto-2014-5>.

147. See O’Hara, *supra* note 20.

elsewhere as a condition of digital access, reinforced by their extraterritorial application, bolstering the Brussels effect. This can be characterized as a liberal rights-based approach. China is also seeking growing influence under the Beijing effect, through which China is shaping transnational data governance through initiatives like the Digital Silk Road, whereby others are offered the tools to emulate China's state-centric, centralized form of data governance and control.¹⁴⁸ This is combined with a strategy of seeking to influence and lead the development and setting of technologies and technological standards, seen most widely in approaches to communications technologies and standards such as 5G and internet systems. Consequently, the competition between different strategies of digital sovereignty between the major economies leads to clashes between them.

1. *Emerging Concepts*

During the past decade, the exercise of sovereignty over the digital world has become a contentious area where governance styles began to collide. While the European Union has been *de facto* the first mover in enacting a cross-sectoral governance framework to curtail the level of control that firms can exercise over the personal data of individuals, the concept of digital sovereignty has been first used to assert the sovereign powers of nation-states. Specifically, reference to “sovereignty” appeared as a point of policy tension between the United States and China.¹⁴⁹ In 2010, following the U.S. “internet freedom agenda”—that extended the freedoms of expression, religious belief, and assembly of the physical world to the internet¹⁵⁰—the Chinese government issued a White Paper in which the internet was defined as a sovereign space—

148. Marie Lamensch, *Authoritarianism Has Been Reinvented for the Digital Age*, CTR. FOR INT'L GOVERNANCE INNOVATION (JULY, 9, 2021), <https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/>; (outlining the development of digital authoritarianism and its characteristics); Erie & Streinz, *supra* note 31 (explaining the use of the Digital Silk Road and One Belt One Road investments as vehicles for transferring data governance approach).

149. Hillary Rodham Clinton, Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>.

150. According to this vision, the internet was to be an “open, interoperable, secure, and reliable” information infrastructure. *See id.*

a matter of national security and public interests.¹⁵¹ These ideational conceptions manifest in different, at times conflicting outputs.

Data sovereignty is evolving as a legal notion to reflect the variety of governance and capitalism embraced by each jurisdiction. As the point of origin of the world's data infrastructure and data economy, the United States has been promoting an open and global market economy for data where sovereignty has been primarily intended as a mechanism to empower market participants and also freedom of expression. The full control over data, exercised through the full alienability of ownership rights over data, has been a central tenet of the data economy that, from the United States, spread throughout a significant portion of the world.

Unlike the United States, the European Union has aimed at achieving digital autonomy to protect both a European rights-based society and the Single Market while supporting competitiveness vis-à-vis the United States and increasingly China.¹⁵² Albeit the term is not deployed uniformly,¹⁵³ digital sovereignty has been outlined as a goal in the visions communicated by the European Commission's Roadmap for the Digital Decade.¹⁵⁴ Moreover, it has been reinforced as an objective by the European Council,¹⁵⁵ European

151. *The Internet in China*, STATE COUNCIL INFO. OFF. (China) (June 8, 2010) http://hk.ocmfa.gov.cn/eng/jbwzlm/xwdt/zt/zfbps/201206/t20120621_10095576.htm.

152. The European Union Agency for Cybersecurity (ENISA) defines digital strategic autonomy as “the ability of Europe to source products and services that meet its needs and values, without undue influence from the outside world.” See EUR. UNION AGENCY FOR CYBERSECURITY (ENISA), CYBERSECURITY RESEARCH DIRECTIONS FOR THE EU'S DIGITAL STRATEGIC AUTONOMY (Apr. 23, 2021), <https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy>.

153. See Circiumaru, *supra* note 141.

154. EUR. COMM'N, EUROPE'S DIGITAL DECADE: 2030 DIGITAL TARGETS (2021), <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12900-Europe-s-digital-decade-2030-digital-targets>; See also 2030 *Digital Compass: the European way for the Digital Decade*, COM (2021) 118 final (Sept. 3, 2021).

155. GER. PRESIDENCY OF THE COUNCIL OF THE EUR. UNION, TOGETHER FOR EUROPE'S RECOVERY (2020), <https://www.eu2020.de/blob/2360248/e0312c50f910931819ab67f630d15b2f/06-30-pdf-programm-en-data.pdf>; Charles Michel, President of the Eur. Council, Digital Sovereignty is Central to European Strategic Autonomy (Feb. 3, 2021) <https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digialeurope-masters-of-digital-online-event/>.

Parliament,¹⁵⁶ the European Union Agency for Cybersecurity (ENISA),¹⁵⁷ and the individual Member States.¹⁵⁸

Of the three major economies, China has advanced the clearest and broadest position on digital sovereignty. In 2017, China released the International Strategy of Cooperation on Cyberspace, highlighting “cyber sovereignty” in the context of extending State-based controls to the digital realm. In such a document, China recognizes the sovereign rights of the national government vis-à-vis other governments, non-state actors, and equality of states via multilateral state-led management of the digital realm versus the current decentralized model.¹⁵⁹ From this general principle flows three objectives:¹⁶⁰ (1) the maintenance of control over the flow of information to preserve the country’s stability; (2) the establishment of technological autonomy; and (3) the creation of a digital realm where the country’s military, political, and economic influence is reflected.

2. *Divergent Scopes*

Digital sovereignty is a central aspect of shaping data governance regimes. In the United States, historically, digital sovereignty has asserted the primacy of private firms, limited only by national security interests. For example, in 2018, the U.S. Federal Communications Commission reclassified internet service providers as information services instead of common carrier services, thus removing net neutrality rules in the United States—allowing ISPs to assign different speeds to different user data flows.¹⁶¹ Yet, in line with the adversarial nature of the U.S. modality of regulation, efforts of federal agencies to control the internet have been curtailed by courts. Law enforcement

156. Tambiama Madiaga, *Digital sovereignty for Europe*, EPRS IDEAS PAPER (July 2020) [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).

157. See ENISA, *supra* note 152.

158. In 2016, Germany and France promoted European digital sovereignty in the Franco-German Council of Ministers. Press Release, Nat’l Cybersecurity Agency of Fr. (ANSSI), *The European digital sovereignty – A common objective for France and Germany* (Apr. 7, 2016) <https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany/>.

159. INTERNATIONAL STRATEGY OF COOPERATION ON CYBERSPACE (Mar. 08, 2017), http://p.china.org.cn/2017-03/08/content_50081017_3.htm (China).

160. See Creemers, *supra* note 109.

161. State rules, however, can supersede the federal rules, though so far only California is enforcing net neutrality.

agencies have tried to seize domain names, in application of the Pro IP Act, allowing the federal government to take control of property suspected of being used in criminal activity.¹⁶² However, courts have limited this interpretation that would have allowed them to take down websites based on summary evidence of criminal activities.¹⁶³ This approach is now clearly evolving under both the Trump and Biden administrations, but as yet with no clear path other than competing with China, maintaining U.S. power, and reducing the power of Big Tech.

In contrast, the European Union aims at protecting consumers, thus, interpreting sovereignty as a system of rights that justifies public intervention in the digital world, like in any other market. Through this prism, the 2017 Consumer Protection Regulation expressly provides regulators within the European Union authority to block ISPs, web hosts, domain registries, and delete websites, even if they are not European.¹⁶⁴ In line with its outcome-based regulatory mode, the European Union intends to incentivize online platforms to align with European values when it comes to business conduct and behavior towards society, as highlighted by the upcoming Digital Services Act package that requires transparency about how online platforms influence user activity.¹⁶⁵ In the European Union, net neutrality is laid down by E.U. Regulation 2015/2120: Safeguarding of open internet access, which is an integral part of the Union's Digital Single Market policy.¹⁶⁶ The law ensures a minimum level of net neutrality in the European Union (and, more broadly in the European Economic Area). However, it also allows for the Member States

162. Specifically, The Pro IP Act 18 U.S.C. §§ 2323. *See generally* Karen Kopel, *Operation Seizing Our Sites: How the Federal Government is Taking Domain Names without Prior Notice*, 28 BERKELEY TECH. L.J. 859, 860-77 (2013) (discussing a trend of US seizures of domain names by the Immigration and Customs Enforcement Office to protect intellectual property rights).

163. *Puerto 80 Projs. v. United States*, Case 1:11-cv-04139-PAC (S.D.N.Y., 4 Aug. 2011) (order denying petition for release of domain names seized by Immigration and Customs Enforcement).

164. *The Internet and Extra-Territorial Effects of Laws*, INTERNET SOC'Y (Oct. 18, 2018), <https://www.internetsociety.org/resources/doc/2018/the-internet-and-extra-territorial-effects-of-laws/>.

165. *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Service Act) and amending Directive 2000/31/EC 2020*, COM (2020) 825 final (Dec. 15, 2020).

166. *See* Harald Øverby & Jan A. Audestad, *Standards, Regulations, and Net Neutrality in the Digital Economy* 26 (May 15, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3601725 (finding net neutrality and other standards as increasingly powerful representatives of regulatory trajectories).

to specify stricter neutrality requirements, allowing the prioritization of specialized services like remote surgery or driverless cars.¹⁶⁷

Finally, China displays a state-centered focus supported by a command-and-control approach. Domestic sovereignty over data and data infrastructure is highly centralized and supported by precise rules with limited room for interpretation by market participants. Concretely, this governance regime works through a combination of regulatory provisions and technological solutions implemented to manage data flows, access and uses within the Great Firewall.¹⁶⁸ Regulators can request private companies to immediately hand over necessary data or block contents.¹⁶⁹ Circumvention technologies, like virtual private networks, are actively interrupted and the government can disconnect companies or whole regions from the internet as necessary.¹⁷⁰

Though Chinese ISPs are not neutral in monitoring and reacting to politically harmful information, commercial network neutrality is becoming a growing policy priority.¹⁷¹ Similarly, there have been ongoing discussions to open cross-border data flows. The Data Security Law stipulates that the government will actively engage and promote “. . . the secure and free flow of data across borders.”¹⁷² This has been reflected in policy documents denoting the establishment of the Hainan Free Trade Port, with a pilot for more liberal

167. *Id.*

168. See JAMES GRIFFITHS, *THE GREAT FIREWALL OF CHINA: HOW TO BUILD AND CONTROL AN ALTERNATIVE VERSION OF THE INTERNET* 22-64 (2019) (investigating examples of how the firewall has been employed on the internet for state purposes).

169. This was for instance the case for WeChat and Weibo, two popular messaging services and social networks. See Adam Segal, *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace*, NAT'L BUREAU ASIAN RSCH. No. 87 (2020).

170. See GRIFFITHS, *supra* note 168.

171. Henry L. Hu, *The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration*, 207 CHINA Q. 523, 523-29 (2011) (discussing the phenomenon of network convergence in the form of growing ISP service standardization in China); Jun Wu & Qingqing Wan, *From Wechat to We Fight: Tencent and China Mobile's Dilemma*, PAC. ASIA CONF. ON INFO. SYS. 265, 265-75 (2014) (while there is a high level of state intervention in data governance, there is still a level of self-regulation in the Chinese market, especially when outside the scope of data content); Meijuan Li & Lei Hou, *Welfare Effects of Network Neutrality in Mobile Internet Market*, 14 ENTER. INFO. SYS. 352, 352-55 (2020) (arguing that net neutrality should be enforced in China for the economic welfare gains).

172. *China's Data Security Law Will Create Dilemmas*, OXFORD ANALYTICA (Aug. 5, 2020), <https://www.emerald.com/insight/content/doi/10.1108/OXAN-DB254376/full/html>; Creemers, *supra* note 109.

cross-border data flows,¹⁷³ or the Shanghai municipal guideline which aims to relax restrictions and generate increasing white lists of companies with direct access to the “international internet.”¹⁷⁴ An example of the free flow of data is the growing connection of banks serving Chinese state-owned enterprises and corporations to the global SWIFT payment messaging networks. At the same time, recent changes mandate both data localization and monitoring of any cross-border flows.¹⁷⁵

In addition, as evidenced by the approach adopted in the European Union and China, digital sovereignty is not limited to asserting control over data and data flows. It also implies the establishment of technological and infrastructural independence. Both jurisdictions aim to reduce (E.U.) or eliminate (China) dependence on U.S. companies and technology. To manage data in the Single Market, the European Union has launched the European Cloud Initiative, to simplify access to data by making it possible to move, share and reuse data seamlessly across European markets and borders.¹⁷⁶ Together with the Franco-German GAIA-X, initiative—a project to connect cloud providers around Europe, harmonize technical standards, and ensure data privacy and security walls—the European Union is creating its own walled garden of data.¹⁷⁷ Federated cloud initiatives are also at the base of ensuring commitment to E.U. values, most recently enshrined in the Berlin Declaration on Digital Society and Value-Based Digital Government.¹⁷⁸ These initiatives reflect the wider strategy to build a secure, high-quality, competitive digital

173. *The Central Committee of the Communist Party of China and the State Council Issued the “Overall Plan for the Construction of Hainan Free Trade Port,”* XINHUA NEWS AGENCY (June 1, 2020), http://www.xinhuanet.com/politics/2020-06/01/c_1126061034.htm.

174. Xiaomeng Lu, *Is China Changing Its Thinking on Data Localization?*, THE DIPLOMAT (June 4, 2020), <https://thediplomat.com/2020/06/is-china-changing-its-thinking-on-data-localization/>.

175. China’s cyberspace regulator recently launched an investigation into one of China’s largest tech companies over an alleged failure to follow personal data collection rules. Josh Horwitz & Yilei Sun, *Explainer: What is Driving China’s Clampdown on Didi and Data Security?*, REUTERS (July 7, 2021) <https://www.reuters.com/technology/what-is-driving-chinas-clampdown-didi-data-security-2021-07-07/>.

176. *Cloud Computing*, EUR. COMM’N, <https://digital-strategy.ec.europa.eu/en/policies/cloud-computing> (last visited Mar. 29, 2021).

177. Konstantinos Komaitis, *Europe’s Ambition for Digital Sovereignty Must Not Undermine the Internet’s Values*, 2021 COMPUT. FRAUD & SEC. 11, 12-16 (2021) (arguing that the internet needs to be retrofitted for modern emerging legal problems).

178. *Berlin Declaration on Digital Society and Value-Based Digital Government*, EUR. COMM’N (Dec. 8, 2020), <https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government>.

infrastructure, without relying on U.S. companies or Chinese data infrastructure vendors.¹⁷⁹

China aims to reduce and ideally eliminate dependence on foreign entities for handling data, as well as providing data infrastructure. A draft measure by the China Banking Regulatory Commission in 2014 called for three-quarters of ICT products in China's banking system to be "secure and controllable" by 2019.¹⁸⁰ The same year, the Chinese government ordered every government office and public institution to remove all foreign software and hardware within the next three years.¹⁸¹ These measures have become explicit in 2020 and 2021 as the result of the new Data Security Law, PIPL, State Council strategy, and other changes appearing to set out an increasingly autarkical trajectory, albeit one which permits and even encourages others to join.

B. EXTRATERRITORIALIZATION AND INTERNALIZATION

In addition to its function of regulating public-private relationships internally, digital sovereignty seeks to support and protect domestic interests in the international arena. This occurs in two manners.

First, through the extraterritorial enforcement of domestic laws, states ensure the application of domestic policies outside jurisdictional borders. Although domestic governance styles may shape the mode of enforcement, extraterritorial application of domestic regimes is essential in the context of data mobility. In 2014, Microsoft challenged an FBI warrant to surrender the

179. Ulrike Franke Torreblanca Carla Hobbs, Janka Oertel, Jeremy Shapiro & José Ignacio, *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry—European Council on Foreign Relations*, EUR. COUNCIL ON FOR. REL. (July 30, 2020), https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/.

180. Zhōngguó yínháng yè jiāndū guǎnlǐ wěiyuánhui guānyú yīngyòng ānquán kě kòng xīnxì jìshù jiāqiáng yínháng yè wǎngluò ānquán hé xīnxì huà jiànshè de zhǐdǎo yìjiàn (中国银行业监督管理委员会关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见) [Guiding Opinions on Applying Secure and Controllable Information Technologies to Strengthen the Cybersecurity and Informatization Construction of the Banking Industry], CHINESE BANKING REGULATORY COMMISSION (Sept. 3, 2014), *translated in* DIGICHINA: STANFORD UNIVERSITY (Sept. 3, 2014), <https://digichina.stanford.edu/work/guiding-opinions-concerning-using-secure-and-controllable-information-technology-and-strengthening-cybersecurity-and-informatization-in-the-banking-sector/>.

181. Yuan Yang & Nian Liu, *Beijing Orders State Offices to Replace Foreign PCs and Software*, <https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406> (last visited Jan. 16, 2023).

emails of a target account stored on a server located in Ireland, claiming that the warrant has no extraterritorial reach.¹⁸² As the U.S. Court of Appeals for the Second Circuit ruled in favor of Microsoft, the Department of Justice filed an appeal with the Supreme Court in 2017, arguing that because Microsoft employees could access the data, they must comply with the warrant.¹⁸³ The case was mooted when Congress introduced the CLOUD Act, allowing enforcement agencies to compel the production of communications content without regard to the location of the data.¹⁸⁴ Beyond the new authority granted by the CLOUD Act, extraterritorial sovereignty is exercised in other areas of data governance. For instance, courts have required internet search engines, web hosting sites, internet service providers, and domain name registries to cease facilitating access to certain content based on IP infringement.¹⁸⁵

The European Union has likewise taken an explicitly extraterritorial approach in recent years, as the GDPR establishes a set of rules for personal data within and outside of the European Union. In particular, unless provided equivalent protections to the data of citizens held inside the European Union, data mobility and related economic activities with the Single Market are prohibited. Moreover, the 2013 Directive on Attacks Against Information Systems extends the notion of a criminal act to the territory where the offense occurs and imparts extraterritorial jurisdiction based on the active nationality principle.¹⁸⁶ The principle applies a jurisdiction's criminal laws to the conduct of its citizen outside the jurisdiction's borders, thereby ensuring extraterritoriality in cybersecurity. Through these initiatives, the European Union also aims to set the standard for the treatment of data, since the implementation of a minimum level of E.U. standards is a precondition to deal with E.U. citizens' personal data.

182. The warrant was provided to the FBI on the basis of the Stored Communications Act. *See* 18 U.S.C. §§ 2701-2712.

183. *See* *Microsoft Corp. v. United States*, 829 F.3d 197, 216 (2d Cir. 2016) (concluding “that Congress did not intend the [Stored Communications Act’s] warrant provisions to apply extraterritorially”).

184. *See* Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348, div. V (2018) (codified in scattered sections of 18 U.S.C.)

185. *See, e.g.,* *Elsevier Inc. v. www.Sci-Hub.org*, 2015 WL 6657363, at *1 (S.D.N.Y. Oct. 30, 2015) (where a judgment prescribed extraterritorial reach of the Copyright Act of 1976, by requiring injunctions of content against alien defendants). For a discussion of the extraterritorial reach, see Jennifer Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9 (2018-2019).

186. *See* INTERNET SOC’Y, *supra* note 164.

Like the United States, China has also established rules authorizing the unilateral extraction of data concerning legal or natural persons being investigated under Chinese criminal law from servers and hard drives located outside of China.¹⁸⁷ Law enforcement agencies are granted the power to extract data via the internet and have established remote network inspection standards to detect criminal activities.¹⁸⁸

Second, sovereignty supports policies aimed at protecting states from internal and external threats. With mounting geopolitical competition, particularly between the United States and China, digital sovereignty has been taking a national security and intelligence character. In more recent years, the U.S. State Department and the Department of Defense formulated the International Strategy for Cyberspace and the Strategy for Operation in Cyberspace in 2011, which set principles for the formation of cyber-alliances and containment of malicious behavior in cyberspace.¹⁸⁹ The U.S. national defense strategy proclaims a “right to self-defense” in cyberspace, explicitly declaring the capability to block or control conflict escalation through network methods as a strategic objective.¹⁹⁰ An expanding policy lexicon imparts the cyber domain with a spatial status similar to that of land, sea, air, and space doctrine, encompassing a need to secure “a freedom of action” in the space, which has a binary inside/outside character.¹⁹¹ Through the Foreign

187. Guānyú bànlǐ xíngshì ànjiàn shōují tíqǔ hé shěchá pànduàn diànzǐ shùjù ruògān wèntí de guǎdìng [关于办理刑事案件收集提取和审查判断电子数据若干问题的规定] (Provisions on Several Issues Concerning the Collection, Extraction, Examination and Judgment of Electronic Data in Handling Criminal Cases) (promulgated by the Sup. People’s Ct., Sup. People’s Proc., and Ministry of Pub. Sec., 2016, effective Sept. 20, 2016) Art. 9 https://www.spp.gov.cn/xwfbh/wsfbt/201609/t20160920_167380_1.shtml (providing for “inspection” of a remote computer information system through the network in case the original storage medium cannot be seized) *translated in* CHINA LAW TRANSLATE (Sept. 20, 2016), <https://www.chinalawtranslate.com/en/provision-on-collection-and-review-of-digital-information-in-criminal-cases/>.

188. *Id.* Remote network inspections on remote computer information systems related to crime include: investigation, discovery, and collection of electronic data through the internet.

189. EXEC. OFF. OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD, (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

190. *Id.* at 9.

191. See Jordan Branch, *What’s in a Name? Metaphors and Cybersecurity*, 75 INT’L ORG. 39, 41-55 (2021) (proposing that foundational metaphors in digital governance are highlighting paradigmatic shifts towards controlling cyberspace).

Intelligence Surveillance Act (FISA), the NSA (National Security Agency) is authorized to perform electronic surveillance of foreign intelligence without warrant.¹⁹² In light of its supranational character, the European Union is limited to a coordinating role in national security matters. While it protects E.U. citizen data from potential surveillance by third countries, as found in the *Schrems II* decision,¹⁹³ the European Union does not prohibit the cyber operations of Member States—which remain outside the E.U. mandate.¹⁹⁴ In China, Cybersecurity Law protects national interests in the digital space. The Cyberspace Administration of China has, for example, enacted regulations banning “fabricating information or inciting extreme emotions” in public internet accounts—regardless of whether the internet account is on a local or extraterritorial website.¹⁹⁵

The assertion of digital sovereignty to defend against internal and external threats supports the growing expansion of national security and defense policies in the digital world. As datafication continues, fewer and fewer sectors remain digitally independent from others. Societal dependencies on digital systems, including the digital economy, public sphere, critical industrial infrastructure, democratic and other governance processes, and even day-to-day societal functions are contingent on digital security.¹⁹⁶ In turn, human and national security are increasingly dependent on the authenticity, availability, integrity, and confidentiality of data.¹⁹⁷ Securing and maintaining control over data, data flows, and data infrastructure are critical for a wide range of policies and to support fundamental societal functions. However, absent an

192. 50 U.S.C. § 1881.

193. Case C-311/18 Data Prot. Comm’r v. Facebook Ireland Ltd., ECLI:EU:C:2019:1145 (July 16, 2020).

194. See Theodore Christakis, *Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)*, EUR. L. BLOG (Apr. 13, 2021), <https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/>.

195. 互联网用户公众账号信息服务管理规定 [Hùliánwǎng yònghù gōngzhòng zhànghào xīnxi fúwù guǎnlǐ guīdìng] (Administrative provisions on the Information Services Provided through Official Accounts of Internet Users) (promulgated by the Cyberspace Administration of China, Jan. 22, 2021, effective Feb. 22, 2021) http://www.cac.gov.cn/2021-01/22/c_1612887880656609.htm translated in CHINA LAWS PORTAL (Jan. 22, 2021), <https://www.chinajusticeobserver.com/law/x/administrative-provisions-on-the-information-services-provided-through-official-accounts-of-internet-users-20210122>

196. See DENARDIS, *supra* note 6, at 131.

197. See DENARDIS, *supra* note 6, at 131.

internationally concerted approach, the jurisdictional securitization of data governance further deepens fractures.

C. DATA SECURITIZATION

Data securitization is a process whereby jurisdictions absorb data governance, or a significant portion of it, within the perimeter of national security and defense policies. The intensity of securitization is scalar rather than binary. In some cases, jurisdictions made exceptional provisions to control the use of data and protect national interests in case of external or internal threats. An example is the “right to self-defense,” set out in the U.S. International Strategy for Cyberspace.¹⁹⁸ In other instances, security concerns permeate domestic data governance. In China, the Cybersecurity Law is a constitutive component of the country’s emerging data governance regime; in the United States, FISA allows the NSA to collect information from foreign firms.¹⁹⁹ Data securitization is, therefore, a process that occurs irrespective of the level of liberalism towards data governance.²⁰⁰ Crucially, steps towards greater securitization of data in one jurisdiction trigger counteractions in others, fueling a progressive absorption of data governance into national security and defense policies. The spatial metaphors to support American cybersecurity,²⁰¹ for example, naturalize the existence of threats and subsequently legitimize reactions, such as the tightening of the controls through the Great Firewall, in China. Interjurisdictional tensions, and interstate cooperation (with allies), are intensifying, thus deepening the fragmentation of global data governance and pushing the formation of “digital Berlin walls.”²⁰²

198. See Lu *supra* note 174.

199. 50 U.S.C. § 1881.

200. Thierry Balzacq, Stefano Guzzini, Michael C. Williams, Ole Wæver & Heikki Patomäki, *What Kind of Theory—If Any—Is Securitization?*, 29 INT’L REL. 96 (2014) (presenting the emerging theory of securitization across various disciplines); Maximiliano Facundo Vila Seoane, *Data Securitisation: The Challenges of Data Sovereignty in India*, 42 THIRD WORLD Q. 1733 (2021) (Using the Indian data governance regime as an example of securitization); Christian Kaurert & Sarah Léonard, *The Collective Securitisation of Terrorism in the European Union*, 42 W. EUR. POL. 261 (2019) (highlighting securitization in the European Union through a case study of counter-terrorism related regulatory efforts).

201. 50 U.S.C. § 1881.

202. Press Release, The White House, The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China (July 19, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/>

In general terms, data securitization processes are evolving along two trajectories. In some cases, policymakers expand the scope of national security rules to include areas that are not traditionally related to national security matters. As the targets of cyber threats extend to a wider variety of organizations and economic actors,²⁰³ so do the parameters of domestic cyber-resilience strategies that now include *inter alia* commerce, communications, individual privacy, finance, and intellectual property.²⁰⁴ As a consequence, intelligence agencies increasingly rely on private sector participants to support their activities. For example, the U.S. PRISM surveillance program secured direct access to communication and stored information from the servers of Microsoft, Yahoo, Google, and Facebook.²⁰⁵ In line with this trajectory, jurisdictions have designed holistic defense strategies that include the digital world.²⁰⁶ The European Union has advanced a comprehensive data securitization package starting with the Cybersecurity Strategy, which coalesces a variety of rules and includes supranational and national intelligence agencies,

2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

203. More than seventy percent of all global companies and organizations are estimated to be subject to virtual attacks, and their frequency is increasing by approximately forty percent every year, with cascading and unpredictable consequences. See WORLD ECON. F. CTR. FOR CYBERSECURITY, ANNUAL GATHERING OF THE CENTRE FOR CYBERSECURITY COMMITTED TO SECURING OUR SHARED DIGITAL FUTURE (2018). For more general discussion on cybersecurity, see NortonLifeLock, *2019 Cyber Safety Insights Report Global Results* (Mar. 30, 2020) (discussing a notable example of cybersecurity risks being the hack of SolarWinds, in 2020 provided hackers access to the data of Fortune 500 companies).

204. For example, the U.S. National Cyber Strategy aims to identify critical function lists that are sensitive to cybersecurity, including national security, energy and power, banking and finance, health and safety, communications, information technology, and transport. THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (2018).

205. For a discussion of the U.S. PRISM program, see generally Alex Marthews & Catherine E. Tucker, *Government Surveillance and Internet Search Behavior* (Mar. 15, 2017) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564; Genna Churches & Monika Zalnieriute, *'Contracting Out' Human Rights in International Law: Schrems II and the Fundamental Flaws of US Surveillance Law*, HARV. INT'L L.J. ONLINE (2020), (discussing how the EU Courts found surveillance programs like PRISM, that collected data directly from undersea cables and providers like Google and Facebook, were necessary for foreign intelligence).

206. See Chooi Shi Teoh & Ahmad Kamil Mahmood, *National Cyber Security Strategies for Digital Economy*, INT'L CONF. ON RSCH. & INNOVATION IN INFO. SYS. (ICRIIS) 1-9 (2017) (discussing the growth of cybersecurity regulation).

law enforcement, defense authorities, and industry stakeholders.²⁰⁷ Within this framework, the European Union established a minimum set of security standards.²⁰⁸ Furthermore, current proposals entail a pan-E.U. authority, the ENISA, with the mandate to increase operational cooperation between the Member States of the European Union and to establish a European cybersecurity certification framework to assess the risks of digital products and services.²⁰⁹

A second policy trajectory departs from the national security and defense paradigm and mandates the implementation of data security systems to private entities for consumer protection.²¹⁰ Cybersecurity provisions are embedded in sector-specific regulatory frameworks. The rules concerning privacy and data protection in the financial sector epitomize this trajectory. The Gramm-Leach-Bliley Act of 1999 compels financial institutions to implement data security requirements to safeguard “security and confidentiality” of customers' records and to protect their systems from unauthorized access.²¹¹ Similarly, in the European Union, the regulatory framework for financial services comprises a

207. Anton Didenko, *Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonisation in the EU and Beyond*, 25 UNIFORM L. REV. 125, 125-35 (2020) (presenting an emergence of cybersecurity regimes in all three jurisdictions discussed in this paper).

208. The Security of Network and Information System (NIS) Directive establishes a baseline that can be overridden by other sectoral rules. *See* Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) /1.

209. The instrument was adopted in its final form in April 2019. *See* Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2019 O.J. (L 151) /15.

210. *See* Zachariah Tyree, Robert A. Bridges, Frank L. Combs & Michael R. Moore, *Exploiting the Shape of CAN Data for In-Vehicle Intrusion Detection*, 2018 IEEE 88TH VEHICULAR TECHNOLOGY CONFERENCE (VTC-FALL) 1 (2018). Jake L. Beavers, Michael Faulks and Jims Marchang, *Hacking NHS Pacemakers: A Feasibility Study*, 2019 IEEE 12TH INTERNATIONAL CONFERENCE ON GLOBAL SECURITY, SAFETY AND SUSTAINABILITY (ICGS3) 206 (2019).

211. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 15 U.S.C.). Additional rules may be applicable, depending on the state. *See, e.g.*, New York Financial Cybersecurity Regulation, N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017). (requiring inter alia for financial institutions to implement “defensive infrastructure” to protect their ITC systems). For an analysis of the regulation, see Jeff Kosseff, *New York's Financial Cybersecurity Regulation: Tough, Fair, and a National Model*, 1 GEO. L. TECH. REV. 432 (2016) (arguing that the New York regulation is a model cybersecurity statute for the United States because it provides an industry-neutral framework).

burgeoning cybersecurity framework, led by the proposal of the Digital Operational Resilience Act, which introduces standardization of security measures, resilience testing, and cross-border cybersecurity oversight for banks in the Union.²¹²

Cybersecurity is a threat to individual state security and digital sovereignty that also impacts the common global data infrastructure. Tensions between individual state objectives and the global commons are increasingly evident, with the potential to result in its fragmentation and fracture.

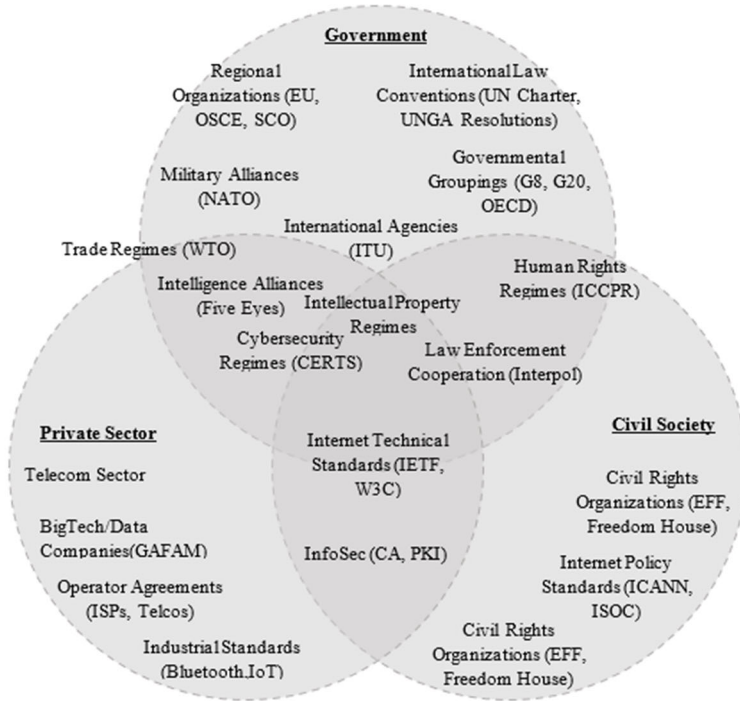
D. THE END OF THE INTERNET AS A GLOBAL COMMONS?

The internet is a network of networks through which most data travels around the world. It is a global commons that connects billions of data-dependent devices into a virtual economy that by itself is among the largest in the world.²¹³ The internet is the lifeline for everything from sending emails, to enabling whole sectors of the global economy, like finance or trade. The incumbent liberal model of the internet is the result of a wide international cyber “Internet Regime Complex”—an interconnected network of international regimes that, through their independent functions, prop up a liberal, permission-less, and open internet.²¹⁴

212. Proposal for a Regulation of The European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM (2020) 595 final (Sept. 24, 2020).

213. The internet has developed the World Wide Web and its superstructural market through a variety of technological advances. *See* Christian Bizer, Tom Heath & Tim Berners-Lee, *Linked Data: The Story so Far*, in SEMANTIC SERVICES, INTEROPERABILITY & WEB APPLICATIONS: EMERGING CONCEPTS 205, 205-21 (2011) (discussing the “Linked Data” that has fostered a revolution in data access and utility); Tim Berners-Lee, James Hendler and Ora Lassila, *The Semantic Web*, 284 SCI. AM. 34 (2001) (presenting the idea of the “Semantic Web” in which data is linked by semantic logic); NAT’L AUDIT OFF., THE UK CYBER SECURITY STRATEGY: LANDSCAPE REVIEW (Feb. 12, 2013) (highlighting that the internet underpins an economy that by itself is in the top five globally).

214. *See* Nye, *supra* note 42.

Figure 1: The Internet Regime Complex²¹⁵

The Internet Regime Complex consists of many separate, yet interlocking governance processes that together define the dimensions of the internet. The private sector provides most of the infrastructure and process data flows across the internet, while major decisions are taken at a government level, with the input of civil society for policy standards. The United States has been instrumental in creating this dynamic. The liberal market nature of the internet, for example, stems directly from the internet's construction upon the U.S. telecommunications regime, which the United States liberalized first domestically and then externally through the General Agreement on Trade in Services (GATS) and other Free Trade Agreements of the World Trade Organization (WTO).²¹⁶ As a consequence, in the incumbent “regime

215. Figure 1 is based on the following works. See Nye, *supra* note 42; Alexander Klimburg & Louk Faesen, *A Balance of Power in Cyberspace*, GOVERNING CYBERSPACE 145, 154 (2020) (promoting a three-part division of internet governance).

216. For a historical perspective on the globalization of telecommunications and the internet, see generally *The Changing Role for Telecommunications in the Economy: Globalisation and Its*

complex,” the role of civil society and other governments in the role of the internet has been limited to technical and soft standards. However, as the U.S.-guided incumbent complex fractures, its derivative model of a unitary internet is similarly fragmenting.

The increasing territorialization of digital space via demarcations of digital sovereignty and data mobility is opening the possibility of a more fundamental fragmentation of the internet, and depletion of the global utility it brings. These dynamics are reflected in the emergence of a multi-centered internet where conflicts permeate each layer of the digital infrastructure.

1. *A Multi-Centered Internet*

While actors, principles, and regulatory approaches define distinctive governance styles, local capabilities have traditionally contributed to the development of the internet at different paces. Cyberspaces have historically been characterized by a center-periphery dynamic, where the United States and (to a lesser extent) Europe have benefited from first-mover advantages, while the South has lagged. The geographical distribution of internet users has been a key factor in the origins of this imbalance, with China experiencing relatively low internet penetration until the early 2000s.²¹⁷ A second factor is represented by the level of development in core infrastructure supporting data flow, with the United States initially significantly more advanced and branching to other continents, particularly Europe, through submarine cables.²¹⁸ Finally, the center-periphery imbalance has been heightened by the concentration in the United States and the European Union of companies engaged in activities that are essential to support the internet, such as the domain name system (DNS) and related servers, which are responsible for routing traffic to specific addresses and websites.²¹⁹ Having the ability to edit the DNS root, these

Impact on National Telecommunication Policy, OECD DIGIT. ECON. PAPERS NO. 11 (1995); DEREGULATION AND INTERDEPENDENCE IN THE ASIA-PACIFIC REGION 415–36 (Takatoshi Itō & Anne O. Krueger eds., 2000).

217. Max Roser, Hannah Ritchie & Esteban Ortiz-Ospina, *Internet*, OUR WORLD IN DATA (2015) <https://ourworldindata.org/internet> (highlighting that by 2005, the United States had seven times more internet users than China).

218. Dwayne Winseck, *Internet Infrastructure and the Persistent Myth of U.S. Hegemony*, in INFO., TECH. & CONTROL IN A CHANGING WORLD: UNDERSTANDING POWER STRUCTURES IN THE 21ST CENTURY 228-60 (2019) (highlighting that there is a relative decline of U.S. hegemony in internet infrastructure from half in 2004, to just twenty-five percent in 2017).

219. The majority of such infrastructure is still dominated by a handful of companies in the United States and Europe. *See generally*, Scott P. Sonbuchner, *Master of Your Domain: Should*

private entities effectively gained the power to remove a nation's internet presence completely while setting the terms of use for accessing the network.²²⁰ Each of these factors resulted in disparities in internet capacity, leaving jurisdictions among the European Union and, to an even greater extent, China, as latecomers with limited influence in the early days of global information technology networks. These imbalances, however, sowed the seed for current fractures.

Recent efforts in China and the European Union to bolster digital infrastructure are seeking to redress, at least partially, the center-periphery dynamic. Yet, as both E.U. and Chinese infrastructure enhancements are occurring with the primary aim of developing an internal market, the center-periphery imbalance is morphing into a multi-centered internet structure with new peripheries. Each major jurisdiction represents a new center, equipped with the adequate infrastructural capacity and a distinctive governance approach. Each center competes to expand its sphere of influence, maximize the benefit of the data economy, and assert sovereignty and influence.

2. *Data Infrastructure Conflicts*

From an analytical standpoint, the internet is a data infrastructure comprising three layers, as suggested in the Benkler-Lessig model: (1) the physical infrastructure layer; (2) the code layer; and (3) the content layer.²²¹ The infrastructure layer forms the physical objects and comprises infrastructures that enable transnational data flows and that collect, store, and process data.²²² This layer links the physical and digital worlds through wires, cables, spectrum, and hardware like computers or routers.²²³ Over 400 fiber-optic submarine cables, myriad microwave devices emitting wireless 4G and 5G, thousands of satellites, balloons, and unmanned aerial vehicles provide access to the internet

the US Government Maintain Control over the Internet's Root, 17 MINN. J. INT'L L. 183 (2008). (arguing that while the Internet Corporation for Assigned Names and Numbers was a semi-private nonprofit organization in California, the US could ensure physical control over internet routing).

220. *Id.*

221. Lawrence Lessig, *THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD* 23-25 (2002).

222. *Id.*

223. *Id.*

across the globe.²²⁴ The second layer encompasses software for the carriage, storage, and delivery of data.²²⁵ It comprises both lower-level software for the carriage, storage, and delivery of data (like the TCP/IP protocol), and higher-level software like operating systems. The content layer encompasses a semantic input that is understandable by end-users via all the materials stored, transmitted, and accessed using the software tools of the previous layer.²²⁶

To ensure cross-border digital connectivity, allowing data flows to move outside domestic borders, there must be a minimum level of harmonization of infrastructures and technical standards.²²⁷ Yet, current trends include the decoupling and the duplication of technological infrastructures, the definition of different technical standards, and the compartmentalization of contents within domestic borders as a result of the emergence of competing, non-interoperable, and increasingly conflicting data governance regimes across major economies, combined with their external export, resulting in fragmentation of transnational data governance. These dynamics reflect profound conflicts that can be observed in each layer of the data infrastructure.

In the first layer (physical infrastructure), the vast majority of infrastructure, like submarine cables, has historically been laid by companies domiciled in the United States. Concurrently, the United States led the creation of regulatory standards for the use and access of the infrastructure, reflecting its open-market policy focus exemplified by the GATS Telecommunications Reference Paper and Agreement on Basic Telecommunications.²²⁸ Together, these documents set out the principles of universal service, licensing, and allocation—stressing, in particular, market access to telecommunications for foreign market participants.²²⁹

These premises and the resulting transnational data governance framework are being challenged by both the European Union and China. The European

224. See L. Chettri & R. Bera, *A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems*, 7 IEEE INTERNET THINGS J. 16, 16-20 (2020) (describing the development of wireless systems).

225. *Id.*

226. *Id.*

227. Pau Puig Gabarró, DIGITAL CONNECTIVITY (2020).

228. Kirsten Rodine-Hardy, *Globalization, International Organizations, and Telecommunications: Globalization, International Organizations, and Telecommunications*, 32 REV. POL'Y RSCH. 517 (2015). (discussing the convergence of the main global telecommunications rules and their adherence to the free market model).

229. *Id.*

Union has taken the upgrade of the existing framework as an opportunity to prevent incumbent market participants' abuse of their dominant position. E.U. policymakers aim to avert the risk that a few large foreign firms would take control over an essential infrastructure to create barriers to entry.²³⁰ As an alternative to the existing system of international negotiation under GATS that would require China to possibly change national telecommunications standards in favor of foreign market participants, it is instead seeking to export a centralized internet structure. Thus, China aims to create a possible parallel digital market based on Chinese-led standards and technology, based on a growing number of submarine cables being branched from Chinese territory.²³¹ These efforts to control information and data flows, internally and externally, have also been implemented via stringent limits imposed on foreign companies operating in the telecommunication sector.

Competition over the control of the infrastructure is also emerging in the context of new technology. Most notably, the implementation of 5G technology—the next generation of wireless mobile technology with greater data speeds, lower latency, and the possibility to connect more devices—is generating new friction. Chinese companies are the largest 5G developers globally, covering close to half of the global 5G networks.²³² The United States and many other partners have chosen to avoid such technology and develop new 5G networks.²³³ The European Union's stance on this matter is not unequivocal, as some Member States view the adoption of Chinese technology favorably.²³⁴

Conflicts in the second layer emerge in the debates concerning the future of the internet. Traditionally, the Internet Corporation for Assigned Names

230. *Joint Statement on Electronic Commerce*, EUR. UNION (July 12, 2018), https://trade.ec.europa.eu/doclib/docs/2018/october/tradoc_157456.pdf (presenting an E.U. proposition to expand the Reference Paper with rules to enhance competitive safeguards in the monopolistic telecommunications market).

231. See Winseck, *supra* note 218.

232. See David Sacks, *China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond*, COUNCIL ON FOREIGN REL. (Mar. 29, 2021), <https://www.cfr.org/blog/china-huawei-5g> (outlining major external investment trends from China in 5G infrastructure worldwide).

233. Madison Cartwright, *Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle*, 9 INTERNET POL'Y REV. 1, 9-12 (2020) (arguing for the emergence of the "geo-economic spaces" based on division of different internet and technology companies).

234. See Sacks, *supra* note 232.

and Numbers (ICANN)—established in 1998 as a not-for-profit entity under California Law and subordinate to the U.S. Department of Commerce—standardized the IP and DNS governance system, setting the fundamental global standards critical to support the data routing systems of the internet. Following a proposal by the European Union and China to strengthen multilateral cooperation, the United States released control of ICANN to the international community in 2016, which internationalized the governance framework.²³⁵ Currently, different positions at the U.N. International Telecommunication Union (ITU) are emerging. China, for example, has proposed a new standard for core network technology named New IP as part of broader efforts aimed at internationalizing its local decentralized internet infrastructure.²³⁶

The content layer is the third and most contentious layer. Companies exert significant market control through operating systems, search engines, and browsers.²³⁷ Embracing liberal data governance, these companies have started collaborating with governmental agencies for various purposes, such as combatting terrorism, economic espionage, and international diplomacy.²³⁸ As a reaction, the European Union and China alike have begun a process of decoupling by building their own higher layers.²³⁹ In China, content is sealed off from the rest of the world by the Great Firewall—a system that turns the Chinese internet into an Intranet, restricting Chinese users from access to the World Wide Web, and keeping foreign users from penetrating the Chinese

235. Danielle Flonk, Markus Jachtenfuchs & Anke Obendiek, *Authority Conflicts in Internet Governance: Liberals vs. Sovereignists?*, 9 GLOB. CONSTITUTIONALISM 364, 364-82 (2020) (presenting a dynamic of different viewpoints regarding the ultimate control of ICANN).

236. See Hoffmann et al., *supra* note 33.

237. Operating systems include iOS, Windows, and Android. The search engine market is dominated by Google. Facebook remains the biggest global social network, Amazon the largest global retailer, and ICANN is domiciled in the United States. For a deeper discussion, see Winseck, *supra* note 218.

238. See Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon & R.B.J. Walker, *After Snowden: Rethinking the Impact of Surveillance*, 8 INTL. POL. SOCIO. 121, 121-35 (2014) (discussing allegations of GAFAM firms handing information on users to intelligence services without their user's knowing).

239. For examples of movements away from GAFAM software, see Matt Hanson, *China to Ditch All Windows PCs by 2022—Could this Be Linux's Time to Shine?*, TECHRADAR, (Feb. 14, 2020), <https://www.techradar.com/news/china-to-ditch-all-windows-pcs-by-2022-could-this-be-linux-time-to-shine>; Wolf Richter, *LEAKED: German Government Warns Key Entities Not To Use Windows & Over Links To The NSA*, BUS. INSIDER, (Aug. 27, 2013), <https://www.businessinsider.com/leaked-german-government-warns-key-entities-not-to-use-windows-8-links-the-nsa-2013-8>.

intranet.²⁴⁰ In the European Union, the upcoming Digital Services Act package is placing more responsibilities on digital service providers to incentivize the establishment of internal mechanisms of compliance, as regulated firms are expecting to cooperate with regulators in achieving stated principles.

As a result of these fundamental conflicts affecting each layer of the data infrastructure from emerging data governance regimes, fractures are increasingly inevitable, and consequences are poised to reshape the role of the internet at the center of data globalization. In particular, transnational data governance is developing along territorial lines, some of which are closed-loop, fragmenting, and potentially fracturing the commons of the internet.

IV. ADDRESSING THE WICKED PROBLEM OF TRANSNATIONAL DATA GOVERNANCE

The fragmented framework for transnational data governance generates a wicked problem. Characteristically, this type of problem features a conundrum, as any solution is only partial and bound to entail new issues. Fragmentation of the global framework for data governance, while increasing transaction costs and hampering the opportunities offered by cross-border data aggregation, undermines the core tenets of globalization. Yet, in a context of competing and conflicting regimes, any solution risks favoring one regime over the others, thereby exacerbating conflictual positions. Rather than one correct solution, this wicked problem can be addressed through different approaches targeting the most problematic aspects. In line with this view, addressing the wicked problem of transnational data governance entails harnessing the benefits of data globalization without undermining domestic sovereign priorities.

After having qualified fragmentation in transnational data governance as a wicked problem, this Section offers an analysis of the possible approaches that can be deployed to address it. The first approach is based on the global riparian system for water rights management. A riparian system for data flows would acknowledge the special status of data at the international level while mandating the coordination of bilateral mechanisms between jurisdictions. The second option consists of a plurilateral approach. In light of the

240. Laura Kirste & Dirk Holtbrügge, *Huawei at Bay? A View on Dependency Theory in the Information Age*, in *HUAWEI GOES GLOBAL* 291 (2020).

advantages brought by large networks of data, regulatory coalitions involving multiple jurisdictions could be established. Leveraging technology interoperability, regulatory coalitions could vary depending on regulatory matters and jurisdictions. The third option entails a multilateral approach. Under the aegis of proposals for a new DBW or DSB, international coordination could be established. We suggest that a combination of these approaches would provide a suitable solution, preventing further fragmentation. In particular, a DSB would offer a soft-law framework similar to those established to maintain financial stability, averting further ruptures in the global data flow, while offering a forum to mediate and resolve conflictual positions.

A. THE WICKED PROBLEM OF TRANSNATIONAL DATA GOVERNANCE

The fragmentation of the transnational governance framework generates a problem for which a clear and univocal solution is unattainable. Similar to climate change—whereby complex ecological chain reactions are intertwined with societal perceptions, political pressures, and economic incentives—transnational data governance requires untangling technological elements, domestic priorities, geopolitical tensions, and economic factors.²⁴¹ Any international solution to support a transnational framework for data governance, while entailing significant social benefits, would require overcoming critical hurdles.

International policy cooperation and coordination are essential to address common challenges. The establishment of internationally concerted rules on digital sovereignty, data securitization, and digital infrastructures would promote certainty on crucial matters, such as cross-jurisdictional data mobility and extraterritorial enforcement of domestic rules. Cybersecurity would also benefit from common standards. In a global economic landscape, trade,

241. See Gary E. Marchant, *Governance of Emerging Technologies as a Wicked Problem*, 73 VAND. L. REV. 1861, 1861-66 (2020) (noting that “the pace of technology development far outstrips the capability of regulatory systems to keep up”); Madeline Carr & Feja Lesniewska, *Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance*, 34 INT’L REL. 391, 392-405 (2020) (comparing IoT and cybersecurity to climate change); Susan Ariel Aaronson, *Could Trade Agreements Help Address the Wicked Problem of Cross-Border Disinformation?*, CTR. FOR INT’L GOVERNANCE INNOVATION, (July 6, 2021), <https://www.cigionline.org/publications/could-trade-agreements-help-address-the-wicked-problem-of-cross-border-disinformation/> (highlighting cross-border data as one of the sources of a transnational disinformation problem).

finance, and commerce would benefit from a safer environment if legal certainty and data integrity is ensured.²⁴² Even where jurisdictions prefer to maintain some level of control, domestic policies, international trade, and supply chains depend on data flows that move across jurisdictions. To achieve a minimum level of policy coordination, however, a common understanding is needed.

As the emerging data governance regimes have shown, the three major economies are solidifying intractable divergences in principal digital regulatory architecture. The U.S. approach encapsulates liberal market capitalism, which underpins the evolution of the internet but clashes with the consumer-centered and rights-based regime of the European Union, and with the increasingly controlled capitalism and state-centered structure deployed by China.

These considerations are not merely hypothetical. Internationally, two dynamics reflect the irreconcilable nature of domestic styles and the impossibility to reach a univocal solution.

First, unilateral approaches to the extraterritorial enforcement of rules alter the global data flows. This dynamic is particularly evident in the stances that the European Union has taken toward China and the United States. The GDPR establishes the principles of adequacy, whereby the transborder flow of personal data outside the Single Market can only occur if a certain level of protection is ensured.²⁴³ In this context, E.U. officials have indicated that the expansive surveillance authority of China may never meet the criteria for adequacy recognition.²⁴⁴ The E.U. rights-based regime has clashed with the American market-based regime: the CJEU has repeatedly deemed the U.S. data protection framework insufficient to ensure adequate protection of E.U. citizen data. In 2016, the CJEU ordered the shutdown of the Safe Harbor

242. On the risks of disruption in the commercial context, see *supra* Section II for a deeper discussion of the Chinese Cybersecurity Law.

243. See Streinz, *supra* note 64 and accompanying discussion in text.

244. Laurens Cerulus, *Europe Eyes Privacy Clampdown on China*, POLITICO, (Feb. 4, 2019) <https://www.politico.eu/article/european-union-eyes-privacy-clampdown-on-china-surveillance-huawei/>.

Program²⁴⁵ in the *Schrems I* judgment.²⁴⁶ This stance was reiterated in 2020, when CJEU halted also the successor E.U.-U.S. Privacy Shield regime, which was a data-bridging mechanism allowing thousands of companies to self-certify for personal data transfer across the Atlantic in *Schrems II*.²⁴⁷ At the core of the dispute was whether U.S. intelligence efforts concerning E.U. citizen data should remain out of the adequacy assessment, finding that they should remain within its scope.²⁴⁸

Second, jurisdictions are deploying competing strategies to extend their influence and control over data infrastructure. The California effect,²⁴⁹ the Brussels effect,²⁵⁰ and the Beijing effect²⁵¹ result in the diffusion of three competing models across the world's jurisdictions. Bilateral tensions are thus amplified, as they take a global stage. This dynamic is particularly evident in the context of the European Union. For instance, jurisdictions that aim to meet the GDPR adequacy standards must follow a specific procedure enshrined in Article 45. Accordingly, adequacy decisions are adopted by the European Commission, taking into account various elements, including general elements, such as “the rule of law, respect for human rights and fundamental freedoms,”²⁵² as well as specific aspects such as the existence of data protection laws,²⁵³ the establishment of dedicated supervisory authorities,²⁵⁴ and the commitment to third countries, international, regional or multilateral organizations for the protection of personal data.²⁵⁵ In aligning with these criteria, jurisdictions seeking recognition for adequacy are required

245. See Churches & Zalnieriute, *supra* note 205 (outlining the consequences of the *Schrems* decision, including halting the EU-US Privacy Shield).

246. Case C-362/14, Maximilian Schrems v. Data Prot. Comm’r, ECLI:EU:C:2015:650 (Oct. 6, 2015). See also, Court of Justice of the European Union Press Release No. 117/15, The Court of Justice Declares that the Commission’s US Safe Harbour Decision is Invalid (Oct. 6, 2015).

247. Case C-311/18, Data Prot. Comm’r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (July 16, 2020).

248. Theodore Christakis & Fabien Terpan, *EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options*, INT’L DATA PRIV. L. (2021). (highlighting the central nature of intelligence data access in E.U.-U.S. legal disputes and negotiations).

249. See HALEY & HALEY, *supra* note 142 and accompanying text.

250. See BRADFORD, *supra* note 23 and accompanying text.

251. See Erie & Streinz, *supra* note 31 and accompanying text.

252. GDPR, *supra* note 22, art. 45(2)(a).

253. GDPR, *supra* note 22, art. 45(2)(a).

254. GDPR, *supra* note 22, art. 45(2)(b).

255. GDPR, *supra* note 22, art. 45(2)(c).

to incorporate core aspects of the E.U. data governance regime, effectively expanding its influence but also reducing interoperability with U.S. and Chinese data governance.²⁵⁶ To juxtapose, under the Beijing effect, jurisdictions are adopting the digital infrastructure of Chinese firms and adopting facets of its command-and-control variants of data sovereignty, which in turn are likely to reduce interoperability with E.U. and U.S. data governance.²⁵⁷

As divergent data governance regimes collide, ensuring both the security of data flows and legal certainty in the global data economy is difficult, if not impossible. While a single solution to the wicked problem of transnational data governance may not be possible, different approaches offer a variety of possibilities.

B. BILATERAL APPROACHES: THE RIPARIAN STATUS QUO

Water, like data, raises transnational concerns. 148 countries share at least one transboundary river basin and three-quarters of the world's nations house a river that crosses a political border.²⁵⁸ Yet, there is no central agreement or international organization responsible for governing water rights. In fact, riparian approaches are naturally diverse, since they entail a wide variety of *sui generis* rules tailored to the needs of the parties involved to govern water rights, ownership, sovereignty, environmental matters, and public-private partnerships.²⁵⁹ The U.N. Watercourse Convention—which has had a gestation period of 50 years and entered into force in 2014—aims to help

256. As of August 2021, the European Commission has recognized the following jurisdictions to provide adequate data protection: Andorra, Argentina, Canada (limited to commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United Kingdom, and Uruguay. In June 2021, South Korea launched the procedure for recognition. See *Adequacy Decisions*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Jan. 5, 2023).

257. Erie & Streinz, *supra* note 31.

258. Rebecca L. Farnum, *Drops of Diplomacy: Questioning the Scale of Hydro-Diplomacy through Fog-Harvesting*, 562 J. HYDROLOGY 446, 447-86 (2018) (presenting a broad extent of stakeholders present in water-right related issues).

259. Joseph W. Dellapenna, *The Evolution of Riparianism in the United States*, 95 MARQ. L. REV. 53, 54-75 (2011) (highlighting the complexity and idiosyncratic development of water rights).

conserve and manage water resources. However, as of today, it has been ratified by only a few dozen jurisdictions.²⁶⁰

The current global riparian governance system is an apt analogy for the emerging fragmentation of transnational data governance. Like riparian governance, transnational data governance is increasingly based on domestic choices that, in turn, reflect distinctive governance styles and are embedded in competing and sometimes conflicting regimes. For instance, in the United States, access to water is not a federal matter; rather states implement different rules based on distinct doctrines for allocating rights.²⁶¹ Among various factors, the approaches adopted in each jurisdiction vary depending on availability, necessity, and sociopolitical considerations characterizing the local constituencies.²⁶² Hence, where water represents a scarce resource, a communitarian approach is favored; whereas, an abundance of water results in a more liberal market for water management.²⁶³ The U.S. approach to data has followed a similar path, dominated by abundance and based on the protection of property rights to create a market for data. Alternatively, the European Union establishes standards for water quality and protection.²⁶⁴ However, each country owns its own water bodies and jurisdictional issues are to be decided, with a unanimous voting mechanism, by the European Council,²⁶⁵ the highest political body of the Union. The E.U. data governance regime presents an equivalent focus on privacy and data protection as fundamental rights. However, unlike in the case of water management, the European Union has

260. Convention on the Law of Non-Navigational Uses of International Watercourses, May 21, 1997, A/RES/51/229, <https://digitallibrary.un.org/record/240629/>.

261. Four general types of riparian doctrines have been observed. Absolute ownership allows water users to withdraw water from land without advance considerations to impacts of adjoining property. Reasonable use requires users to obtain a permit based on an evaluation of the reasonableness of the proposed beneficial use. Correlative rights grant water users rights in proportion to their land ownership or other allocation mechanisms. Prior appropriation water use rights are granted based on the timing of the appropriate to access water. *See* Dellapenna, *supra* 259.

262. The right to water is also a U.N. Sustainable Development Goal. On water as a right, see generally Sadia A. Jame & Laura C. Bowling, *Groundwater Doctrine and Water Withdrawals in the United States*, 34 WATER RES. MGMT. 4037 (2020).

263. *Id.*

264. Juliane Albrecht, *The Europeanization of Water Law by the Water Framework Directive: A Second Chance for Water Planning in Germany*, 30 LAND USE POL'Y 381, 381-95 (2013) (highlighting the complexities of water right regimes in the European Union).

265. DIRECTORATE-GENERAL FOR EXTERNAL POL'YS, EUR. PARLIAMENT, CONFLICT AND COOPERATION OVER WATER - THE ROLE OF THE EU IN ENSURING THE REALISATION OF HUMAN RIGHTS (2015).

been moving to establish a pan-E.U. system, where data is a common (and strategic) interest of the Union and its members. Finally, in China, the State owns the water and sets water rights via local governments and through water rights permits for local companies.²⁶⁶ Similarly, data governance is now being centralized with State control and even ownership.

The parallel between data governance and the riparian system of water rights also explains transnational dynamics. First, global data flows have emerged as a part of a global network. Every user, public or private actor, connected to the internet is accessing digital data, and the broader pool of knowledge and information therein contained; similarly, people and entities connect to a shared body of water. Second, from a governance standpoint, competing and conflicting domestic interests restrain access to shared resources. In the same way alterations to a body of water upstream have consequences on communities living downstream, divergent data governance regimes implemented to reflect domestic idiosyncrasies have an impact on other jurisdictions and economies. As a result, international disputes arise but they are commonly resolved through bilateral mechanisms.²⁶⁷

Through this prism, a riparian approach to transnational data governance rests on two pillars. First, it suggests that, in the emerging fragmented framework, bilateralism is the most viable approach. Data governance, like water management, can remain anchored to a framework where different data-flow relationships are established on a case-by-case basis between different jurisdictions and actors. However, owing to the strategic importance of data, a second pillar is necessary to ensure that bilateralism does not deepen existing fractures. Like water, data can be awarded special status in international law. Even without a global framework for water management, jurisdictions have

266. David J. Devlaeminck & Xisheng Huang, *China and the Global Water Conventions in Light of Recent Developments: Time to Take a Second Look?*, 29 REV. EUR., COMPAR. & INT'L ENV'T L. 395, 395-410 (2020) (outlining the different approaches to water rights between China and other countries); Dajun Shen, Ali Guna & Xiaodan He, *Water Use Control System in China*, 36 INT'L J. WATER RES. DEV. 590, 590-601 (2020) (highlighting a state-centered water rights regime in China).

267. For example, there is an ongoing discussion about the diversion of water away from the Illi and Irtysh rivers between China and Kazakhstan. *See generally* Hongzhou Zhang & Li Mingjiang, *China and Global Water Governance*, in CHINA & TRANSBOUNDARY WATER POLS. ASIA (2017) (presenting an exhaustive discussion of water rights regimes and related discussions in Asia).

approached water as a vital resource that transcends policy compartments. In international discussions, water has been traditionally considered a commodity, but significant policy shifts have occurred in the past decade. In 2010, the United Nations passed a resolution explicitly recognizing access to water as a human right, that plays a crucial role in climate policy discussions.²⁶⁸ In a similar vein, the special status of data, data flows, and data infrastructure could be recognized in international conventions to provide the basis for dispute adjudication and, possibly, minimum harmonization or a soft-law framework could be established to create standards to facilitate global cross-border data flow in different domains and, over time, establish a mechanism for the resolution of conflictual relationships.²⁶⁹ Such approaches could be multilateral or plurilateral.

Conversely, a development trajectory following the riparian approach may also highlight the non-issue of the wicked problem. If fragmentation of data governance continues without cutting apart the growing data economy, fragmentation may just highlight the development of more niched, independent, and isolated sub-aspects of what, until now, has been a single mixed pot of state, market, and individual activities in cyberspace. The assertion of control over new data activity by jurisdictions via a riparian mixed-approach may thus be more indicative of rising complexities in data, rather than fragmentation.

C. PLURILATERAL APPROACHES: REGULATORY COALITIONS

A plurilateral approach could build on and expand the riparian approach to transnational data governance. Coalitions of jurisdictions based on sector-specific areas could be created with the intent of having uniform legal and regulatory treatment for sector-specific matters. This approach recognizes and legitimizes the existence of multiple data governance regimes. A jurisdiction may be part of different regulatory coalitions at the same time, depending on the types of data concerned, their use, and destination. For instance, data could

268. See Dellapenna, *supra* note 259; Emanuele Fantini, *An Introduction to the Human Right to Water: Law, Politics, and Beyond*, 7 WIRES WATER 1, 1-8 (2020) (arguing that in spite of United Nations recognition of the human right to water, it is a contested notion in regards to scope, content, and indicators).

269. See generally Bradley C. Karkkainen, *Multi-Jurisdictional Water Governance in Australia: Muddle or Model?*, in REFORMING WATER L. & GOVERNANCE: FROM STAGNATION TO INNOVATION IN AUSTRALIA 57 (Cameron Holley & Darren Sinclair eds., 2018) (presenting the challenges of managing shared basins of water).

follow different rules depending on the applicable regulatory coalition, as the same type of data can be used in trade, law enforcement, or knowledge contexts.

As current experience with adequacy standards has shown, regulatory coalitions entail the establishment of minimum standards. These standards can vary in degree of complexity, from broad adequacy regimes that would ascertain the fit of legal frameworks, like the GDPR, to much more nuanced systems of independent fiduciary data intermediaries that would grant permission for data flows to jurisdictions, private actors, and individuals alike depending on the type of data, their use, and related adequacy.²⁷⁰ A prerequisite of this approach is that coalitions operate through a common set of technical rules within the same network.²⁷¹ In this scheme, a range of legal structures could provide the format of the intermediary.²⁷² Under the data trust model, legal trusts would be created to hold transferable data packages, in which fiduciaries manage what the data is used for and who has access to it for their client.²⁷³ Trusts would hold data across jurisdictions, and offer a variety of risk appetites and management structures, allowing pre-authorized pools of data to be sent to appropriate third parties.²⁷⁴

Such a network could be used for both public and private actors. For example, jurisdictions could agree on networks of rules establishing how and what data can be transferred and through which channels. A variety of technologies are already available to help secure such messages, from DLT and blockchain applications to security-by-design solutions that can help guarantee

270. See Bruno Carballa Smichowski, *Alternative Data Governance Models: Moving Beyond One-Size-Fits-All Solutions*, 54 *INTERECONOMICS* 222, 222-30 (2019) (presenting different forms of fiduciary data trusts as a model for maintaining and sharing data).

271. *Id.*

272. *Id.*

273. Sylvie Delacroix & Neil D Lawrence, *Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 *INT'L DATA PRIV. L.* 236, 236-47 (2019) (arguing that data trusts are key to enable different stakeholders to secure control over their data).

274. Other forms of data governance archetypes are closed, single source, data clearinghouse, data pool, and distributed. In a closed system, there is no sharing between data users and data holders. In a single source system, data holders receive data directly from data users. In a data clearinghouse system, there is an intermediary through which data holders can provide data to data users. In a data pool system, data holders pool data to an intermediary, which data users can access. The intermediary also reverts data to original data holders from the data users. In a distributed system, data holders and data users are intermingled. *See id.*

security of transmissions medium, to AI that can rapidly analyze the content of transmitted data. Private stakeholders could also create their own domain-specific networks. For instance, the SWIFT system of payments messaging could take part in this system. Data from local banks could be transmitted to a central standardized unit to automatically process and determine whether data is allowed to route through a given jurisdiction.²⁷⁵

Through regulatory coalitions, the issue of multiple internets is institutionalized with a technological solution that allows different interests and divergent regimes to coexist. Leveraging on existing networking technologies—that must be implemented in all jurisdictions—multiple sub-networks, with their own levels of permission, are branched together. This system would allow stability and security of the digital world,²⁷⁶ without compromising the ability of individual entities and jurisdictions to determine levels of access.

Central to the plurilateral approach of regulatory coalitions is the existence of a shared network built to bolster the capacity to collect, store, process, and otherwise manipulate data. Within such a network, domestic idiosyncrasies are respected. Hence, regulatory coalitions can facilitate bilateral approaches to transnational data flows (based on a riparian approach), plurilateral regulatory systems, or offer the backbone for a truly multilateral approach, in the context of a new hard law DBW or a soft law DSB.

D. MULTILATERAL APPROACHES: A NEW (DIGITAL) BRETTON WOODS?

The lack of international fora to negotiate differences among regimes and calibrate rules offers a fertile ground for conflictual positions to escalate. In this context, the WTO—within the international framework set out by the GATS—represents the natural venue to define rights and obligations on data flows as well as core regulatory principles applicable to different types of data. To date, however, WTO members have not made specific commitments in this regard,²⁷⁷ and the suitability of the WTO as an effective forum is in doubt. Outside the WTO, a new multilateral approach could be envisaged.

275. This system is similar to the Qualified Trust Service Providers established by the E.U. Second Payments Services Directive that certifies digital ID certificates by pinging back to domestic authorities.

276. DENARDIS, *supra* note 6.

277. Chu & Lee, *supra* note 129.

The divergent, competing and increasingly conflicting trajectories of data governance can aptly be compared to the international financial system in the first half of the twentieth century. Between the beginning of the First World War, in 1914, and the end of the Second World War, in 1945, the global financial system was fractured. Rampant currency devaluation leading to “beggar thy neighbor” policies, together with inconsistent cross-border trade rules and exclusionary trade blocs resulted in the breakdown of the transnational financial system and trade flows.²⁷⁸ Following the end of the Second World War, in 1945, these problems led to the establishment of the Bretton Woods system, a multilateral framework to ensure monetary and financial stability. The Bretton Woods system was a hard law system, a treaty-based framework supporting cross-border interactions among fragmented financial and economic systems via the establishment of the International Monetary Fund (IMF) and the International Bank for Reconstruction and Development, which today is part of the World Bank Group. The aim was to promote global trade and to finance postwar reconstruction through fixed exchange rates and loans supporting economic recovery. As the global data economy is beset by similar instabilities in the context of post-pandemic recovery,²⁷⁹ the model offers a possible blueprint to address the wicked problem of transnational data governance. Broadly, this idea has been framed as a new Bretton Woods—or a DBW—consisting of a general framework for transnational data governance based on a common set of rules.²⁸⁰

Such an overarching global framework would aim to offer a global paradigm for data governance, that is equipped to address the challenges of the Fourth Industrial Revolution. A DBW—like its analog-native predecessor—would stabilize the development of global infrastructures, and support the enactment of new legal rules and regulatory standards. Its role would dovetail with and support the shift from an industrial to a knowledge-

278. Thilo N. H. Albers, *Currency Devaluations and Beggar-My-Neighbour Penalties: Evidence from the 1930s*, 73 *ECON. HIST. REV.* 233, 233-41 (2020) (arguing that unilateral currency depreciations and trade blocks came at a high price to trade and finance).

279. *See generally* INTERNATIONAL MONETARY AND FINANCIAL LAW: THE GLOBAL CRISIS (Mario Giovanoli & Diego Devos eds., 2010) (presenting a broader discussion on the breakdown of the Bretton Woods monetary system and highlighting that its creation as well as breakdown was caused by crises).

280. *See* Medhara & Owen, *supra* note 38.

based global economy, where local and regional economic systems generate, collect, and protect information. Such a structure could be built on existing international initiatives. For instance, the recently formed E.U.-U.S. Trade and Technology Council—aiming to set high-level cooperation towards technology standards, supply chains, security, and competitiveness across the shores of the Atlantic—represents a stepping stone in this direction.²⁸¹ If its membership is extended, a global forum could be established. If its membership remains limited, it is likely to be the model for plurilateral approaches going forward.

As proposed, a DBW would achieve its objectives through three main functions.²⁸² Its primary function would be to provide a coordination mechanism, allowing the market-based United States, rights-based European Union, and state-centric China to hold a regulatory dialogue. Given the expanding tendency of the governance styles of these three jurisdictions, a coordination mechanism on key regulatory matters, such as competition, data mobility, and data securitization, would reverberate across the world regardless of whether jurisdictions decide to adhere to a given style or adopt a given regime, implement a local solution, or are still exploring different options. Beyond this key function, a DBW would also provide a forum where nascent challenges can be addressed. For instance, fundamental agreements on ethical principles concerning the use of data by algorithms and artificial intelligence is unlikely to be solved bilaterally (through a riparian system) or in a plurilateral manner (through regulatory coalitions). Second, the DBW would oversee negotiations over data-related agreements. Based on a set of core principles governing the interoperability of data flows for essential services—such as finance, law enforcement, and public health—a DBW could assist discussions on various international initiatives, including the current debates over the establishment of a global tax regime for digital services.²⁸³ Third, a DBW could perform a legal and regulatory harmonization function.

281. Press Release, Eur. Comm'n., EU-US Launch Trade and Technology Council (June 15, 2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990.

282. See Medhara & Owen, *supra* note 38.

283. This framework would expand and take ownership of existing initiatives like the OECD/G20 Inclusive Framework on Domestic Tax Base Erosion and Profit Shifting. For a general discussion, see generally Veronika Solilová, Danuše Nerudová & Marian Dobranschi, *Profit Shifting and Tax Base Erosion in the Twenty-First Century*, in PROFIT SHIFTING & TAX BASE EROSION 9 (2021) (providing background to the inclusive framework on profit shifting and tax base erosion).

The DBW would also entail core organizations. As the digital divide is hindering development and growth, the hiatus between centers and peripheries must be addressed through dedicated programs of technical assistance and capacity building, supporting jurisdictions to develop and leverage their digital infrastructures through knowledge transfers. These new roles can be performed in coordination with existing multilateral organizations, such as the World Bank and the IMF. A novel, treaty-based framework, however, is hard to be implemented and, as history has shown, critical challenges have ultimately led to enacting a decentralized global financial system.²⁸⁴ In this context, a global framework for transnational data governance can be established as a soft-law system.

In particular, a soft-law institution can be established as a functional twin institution to the Financial Stability Board,²⁸⁵ focused on the stability of global data flows.²⁸⁶ Such an entity, the DSB, may be part of the DBW or operate as a soft-law entity initiated by the G20, as is the case for the Financial Stability Board. It would have three main responsibilities. First, it would represent the engine to promote legal and regulatory harmonization, coordinating the development of policies, principles, and standards across the most salient areas of data governance.²⁸⁷ Against a shared core of rules and principles, jurisdictional and regional adjustments and variations could be implemented to reflect different priorities and needs.²⁸⁸ Second, the DSB would perform a monitoring role, assessing the vulnerabilities arising from the use of data-based

284. Though the Bretton Woods monetary system provides a model for an umbrella policing of transnational governance, the system also proved to have significant limits and was displaced by decentralized global financial markets. *See generally* INTERNATIONAL MONETARY AND FINANCIAL LAW, *supra* note 279, at 8-35 (presenting a broader discussion on the breakdown of the Bretton Woods monetary system, highlighting that its creation as well as breakdown was caused by crises—typical of most changes in international financial law regimes).

285. The Financial Stability Board was set up to find common regulatory ground among the global banking and insurance industry and cover regulatory gaps after the global financial crisis.

286. Robert Fay, *Digital Platforms Require a Global Governance Framework*, CTR. FOR INT'L GOVERNANCE INNOVATION (Oct. 28, 2019), <https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework/>.

287. *Id.*

288. Typically, domestic approaches may diverge on the treatment of social media content and competition policies.

technologies to recommend possible course of actions.²⁸⁹ This activity may be performed in cooperation with the ITU, the Institute of Electrical and Electronics Engineers, ICANN, and other organizations.²⁹⁰ Finally, the DSB would provide a critical information hub, providing aggregate information and statistics on data governance and flows. For instance, more accurate data would be available to domestic authorities regarding the data treatment of large platforms—such as GAFAM and BATs. In a similar vein, organizations like the WTO and the IMF could benefit from the information gathered by DSB to modernize their rules and policies to better meet the needs of the data economy.

While a DBW would offer a suitable framework to address the wicked transnational data governance problem, its implementation presents some difficulties. In particular, an international consensus must be reached to establish such a system. Its operability would ultimately depend on the level of cooperation, with a G20 centered soft law DSB much more likely to be possible at least initially than a full multilateral agreement.

V. A PATH FORWARD?

In this Article, we have considered the wicked problem of transnational data governance. This wicked problem stems from the interaction of increasingly different, competing and conflicting data governance regimes fragmenting the global framework that underpins transnational data flows and the global data economy. Left unaddressed, the wicked problem risks regressing transnational cooperation in any area that benefits from unrestrained data flows. This is a significant risk in the face of both the benefits that global digital commons entail and the dangers posed by digital threats to the international community. These risks have been dramatically increased as a result of the invasion of Ukraine.

Our contribution is threefold. First, we provide a systematic identification of challenges arising from the emerging fragmentation of transnational data governance and data globalization. Second, we develop a comprehensive

289. See Fay, *supra* note 286.

290. A DSB could also help unite a variety of private organizations that have risen in recent years to address pressing challenges, such as the International Grand Committee Against Disinformation, which unites experts sharing recognition of online platforms, or the Global Partnership on AI.

analytical framework to understand the emergence of governance styles and the ensuing materialization of conflicting regimes in the United States, the European Union, and China. This, in turn, allows us to assess the depth of the impact that a fragmented framework for transnational governance has on global data flows. Third, we show the wicked nature of such a problem, for which there is no definitive solution. Instead, we offer three lanes of approaches—entailing bilateralism, plurilateralism, and multilateralism—that could be adopted by the international community to facilitate cross-border data flow, while minimizing clashes with domestic interests.

Moving from our investigation, a series of actionable conclusions can be drawn. First, a balanced combination of the three approaches appears to be a more palatable way to address the transnational data governance problem than their discrete application; in fact, it is a necessity. In consideration of the ongoing competition, offering the ability for jurisdictions to choose—and most importantly, switch—between data governance styles is essential to de-escalate tensions, promote sectoral cooperation, and pave the way for mending fractures in the global flows of data. Moreover, in the current geopolitical context, bilateralism is the most practical and likely starting point, with plurilateralism gradually evolving along with a truly multilateral system. As data becomes a key priority for trade and other transnational policies, plurilateral approaches are a natural evolution to leverage the benefit of larger networks. Sectoral coalitions are likely to increase support for global finance and international trade. Yet only a multilateral approach allows ensuring a minimum level of coordination, even respecting domestic idiosyncratic preferences. At the very least, it would create a single point of reference for handling conflicts in international data flows. While which combination of the three approaches will emerge is yet to be seen, current trends indicate the reinforcement of plurilateral and multilateral approaches.

Through this prism, the second crucial point that our investigation reveals is the necessity to steer away from an uncoordinated bilateral system. Plurilateral approaches to transnational data governance allow data actors such as states, businesses, or individuals to draw on the benefits of the economies of scale. Especially in the digital economy, the availability and frictionless access to data—even without ownership or exclusive control—is becoming increasingly important. Relatively frictionless data travel or access is a necessity

to ensure the efficient functioning of a number of critical networks. For example, SWIFT depends on the ability of banks to receive and send messages across several entities before payment is confirmed. Hence, sectoral coalitions—with adequacy requirements similar to those implemented in the European Union through the GDPR—may leverage existing initiatives where data circulates freely among participating jurisdictions for specific purposes. Current trends in global finance envisage the establishment of data-exchange systems between banks and law enforcement agencies to combat money laundering activities. Similarly, as an increasingly large pool of stakeholders need to be connected to a single network to verify data on trade, goods, services, and parties, major emerging platforms that support supply-chain finance would benefit from regulatory coalitions. Regulatory coalitions might also be the only solution for economies or sectors where data is not available, or access is limited. Connecting to a larger network becomes essential for developing AI applications.

Following this trajectory, plurilateral data governance coalitions are likely to shape the majority of transnational data governance relationships. As public and private actors are likely to seek access to several coalitions at once, multiple adequacy requirements must be met, and their compliance needs to be ensured across different networks. The ability of jurisdictions to switch among a variety of fragmented and disconnected transnational frameworks provides a strong incentive to establish a formal body that both oversees the integrity of the shared network and facilitates the negotiation of any contentious matters. A DSB could perform this role.

Finally, and more broadly, a third conclusion can be drawn highlighting the importance of a DSB that represents a vital component of any solution. The development of legal, regulatory, and technical standards can support bilateral arrangements for data flow, plurilateral networks, and multilateral systems. A DSB, at the most basic level, can identify best practices and minimum requirements in a variety of fields, from cybersecurity and ethical use of AI to protocols for data transfer. At a more advanced level, it may act as a neutral clearing channel (at least) for critical data.

The result is a balanced transnational governance framework that does not require a complete de-fragmentation of the transnational data governance, nor does it require a treaty-based DBW. Instead, it empowers jurisdictions to choose their data governance relationships by providing a standardized

method for opening, closing, and swapping between data channels and regimes. Flexibility and data circulation are, thus, ensured, even in the case of multiple internets, given that this system could manage an increasing amount of connecting and disconnecting transnational data networks.

POLICING POLICE TECH: A SOFT LAW SOLUTION

Barry Friedman[†], *Farhang Heydari*^{††}, *Max Isaacs*^{†††} & *Katie Kinsey*[‡]

ABSTRACT

Policing agencies are undergoing a rapid technological revolution. New products—with almost unfathomable capacities to collect, store, monitor, and transmit data about us—constantly are coming to market. In the hands of policing agencies, some of these products may promise real benefits to society. But too often these public safety benefits are unproven. And many of these products present real harms, including risks to privacy, freedom of speech, racial justice, and much more. Part of “public safety” is being safe from these harms as well.

Despite these risks, new policing tech products continue to be adopted and deployed without sufficient (or any) regulatory guardrails or democratic oversight. Legislative bodies are reluctant to adopt traditional “hard law” regulation. And because there is no regulation, what we are left with is a “race to the bottom” in which policing technology vendors develop increasingly intrusive products with minimal or no safeguards.

This Report explores a “soft law” approach to dealing with the race to the bottom around policing technologies. Specifically, it examines the viability of an independent certification body—governmental or not-for-profit—that would perform both an efficacy review and an ethical evaluation of vendors’ policing technology products, assessing them along privacy, racial justice, and civil rights and liberties dimensions, among others. It explains how, in theory, certification can overcome some of the obstacles facing hard law regulation. It then discusses the practical design considerations that a policing tech certification system would have to navigate. It also surveys the challenges posed in the implementation of a certification regime, including how to ensure the body is legitimate and obtains stakeholder buy-in, and whether certification would encourage or undercut hard law regulation. Ultimately, the Report

DOI: <https://doi.org/10.15779/Z38M90242H>

© 2022 Barry Friedman, Farhang Heydari, Max Isaacs & Katie Kinsey.

† Jacob D. Fuchsberg Professor of Law, Affiliated Professor of Politics, and Founding Director, Policing Project, New York University School of Law.

†† Executive Director, Policing Project, New York University School of Law.

††† Staff Attorney, Policing Project, New York University School of Law.

‡ Staff Attorney, Policing Project, New York University School of Law.

For their many helpful comments and suggestions, we are grateful to our convening participants, Elizabeth M. Adams, Meredith Broussard, Richard Vorder Bruegge, Brandon Buskey, Albert Fox Cahn, Rumman Chowdhury, Cynthia Conti-Cook, Laura Cooper, Catherine Crump, Mary D. Fan, Lori Fena, Joe Ferguson, Andrew Guthrie Ferguson, Christopher Fisher, Jerome Greco, Daniel Kahn Gillmor, Donald Gross, Brian Hofer, Yasser Ibrahim, Lassana Magassa, Ben Moskowitz, Alex Pasternack, Fabian Rogers, Ravi Satkalmi, John Singleton, Mona Sloane, Danyelle Solomon, Vincent Southerland, Katherine Jo Strandburg, Suresh Venkatasubramanian, Doron Weber, Rebecca Ulam Weiner, Michael Wilt, Deborah Witzburg. For their invaluable insight, we additionally are grateful to the various stakeholders we interviewed for our research. For their research assistance, we also thank Brandon Vines, and Nick Tonckens. This work was produced with the generous support of the Alfred P. Sloan Foundation.

concludes that although adopting a certification scheme presents challenges, the idea has enough merit to receive serious consideration as part of a unified system of getting policing technologies in check.

TABLE OF CONTENTS

I.	INTRODUCTION	703
II.	DEFINING THE PROBLEM	708
A.	THE POLICING TECH LANDSCAPE: WIDESPREAD USE, UNQUANTIFIED BENEFITS AND HARMS.....	708
B.	THE ACCOUNTABILITY GAP	713
1.	<i>The current hard law landscape.....</i>	713
a)	The limited constraints of constitutional judicial review	713
b)	Current legislative approaches: few and far between	714
c)	Administrative body regulation: exceptions rather than rule	716
2.	<i>Obstacles facing hard law regulation of policing technology</i>	717
a)	Pacing Problem.....	717
b)	An Information Gap.....	718
c)	An Expertise Gap.....	719
d)	A Public Choice Problem	719
e)	Federalist Fragmentation	720
C.	THE RESULTANT RACE TO THE BOTTOM	721
III.	PRODUCT CERTIFICATION AS PART OF THE SOLUTION? ..	722
A.	WHAT WE'RE EXPLORING	722
B.	COMMON CERTIFICATION EXAMPLES.....	723
C.	CERTIFICATION FOR POLICING TECHNOLOGY: ABSENCE AND DEMAND.....	724
D.	CERTIFICATION AS AN ANSWER TO KEY POLICING TECHNOLOGY GOVERNANCE CHALLENGES	727
1.	<i>Supplying Information and Expertise to Foster Democratic Accountability.....</i>	727
2.	<i>Evading Hard Law Challenges to Curb the Race to the Bottom.....</i>	728
E.	THEORIES OF CHANGE	729
IV.	DESIGN CHOICES.....	731
A.	PRESCRIPTIVE VS. DESCRIPTIVE.....	731
B.	EVALUATING EFFICACY	735
C.	"USE" CASES	739
1.	<i>Don't address use cases.....</i>	740
2.	<i>Certify products, addressing use cases indirectly through product design....</i>	740

3. <i>Directly certify use cases</i>	741
D. SUBSTANTIVE DESIGN STANDARDS	742
E. INSTITUTIONAL DESIGN OF CERTIFICATION ENTITIES	744
F. PUBLIC OR PRIVATE.....	746
V. CHALLENGES.....	748
A. GAINING LEGITIMACY AND CREDIBILITY: PUBLIC BUY-IN.....	748
B. ACHIEVING UPTAKE: AGENCY AND VENDOR BUY-IN.....	749
C. COMPLIANCE AND ENFORCEMENT.....	751
D. FENDING OFF REGULATION.....	752
E. NORMALIZING TECHNOLOGIES	754
F. CREATION OF A CERTIFICATION MARKET	755
VI. CONCLUSION.....	755

I. INTRODUCTION

Deep below Piccadilly Circus, beyond a maze of underground corridors, lies the Westminster CCTV Control Room. A wall of television monitors offers visitors an intimate view of London city life, from the tony boulevards of Belgravia to the bustling streets of Chinatown. With a few clicks, operators can rotate the cameras 360 degrees and zoom nearly 250 feet; the cameras can even detect the movement of a package inside of a car from three blocks away.¹

Martin O'Malley was impressed. Like thousands of other officials from around the world, the Mayor of Baltimore had made the pilgrimage to London to observe one of the most advanced CCTV systems in existence, in one of the most surveilled cities in the world. The previous year, 2003, Baltimore City had recorded over 11,000 violent crimes, making it the seventh most violent city in the United States.² O'Malley had a problem, and the Brits, it seemed, had hit upon a solution.

The idea was simple. CCTV would serve as a “force multiplier”—a single operator in a CCTV control center could perform the work of many police officers, surveilling multiple neighborhoods simultaneously.³ Moreover, the

1. See Paul Lewis, *Every Step You Take: UK Underground Centre That Is Spy Capital of the World*, THE GUARDIAN (Mar. 2, 2009), <https://www.theguardian.com/uk/2009/mar/02/westminster-cctv-system-privacy>; John Buntin, *Long Lens of the Law*, GOVERNING (Mar. 24, 2010), <https://www.governing.com/archive/long-lens-of-the.html>.

2. See NANCY G. LA VIGNE, SAMANTHA S. LOWRY, JOSHUA A. MARKMAN, ALLISON M. DWYER, URBAN INST., EVALUATING THE USE OF PUBLIC SURVEILLANCE CAMERAS FOR CRIME CONTROL AND PREVENTION 23(2011), https://www.urban.org/sites/default/files/publication/27556/412403-evaluating-the-use-of-public-surveillance-cameras-for-crime-control-and-prevention_1.pdf.

3. *Id.*; see Buntin, *supra* note 1.

visibility of the cameras would serve as a deterrent to would-be offenders. Announced in 2005, Baltimore's "CitiWatch" program would become one of the most ambitious CCTV programs in the United States.

Any new surveillance system courts some controversy, but officials had a plan. They held a series of public hearings, assuring citizens that the new cameras would be used judiciously. The Baltimore Police Department implemented a new electronic surveillance policy governing the use of technologies like CCTV. These efforts helped earn the buy-in of Baltimore residents, many of whom initially expressed concern that the CitiWatch program would infringe on their privacy.⁴

As democratic engagement around police surveillance goes, so far so good.

Then came Freddie Gray. The 2015 death of a 25-year-old Black man in the back of a police van sparked protests across the city. In the ensuing civil unrest, 350 businesses were damaged, 150 vehicles were set ablaze, and over a hundred police officers were injured. The Baltimore Uprising, as it came to be known, culminated in "the most extensive rioting in Baltimore since the 1960s."⁵

Soon after, local aviation enthusiasts began noticing planes making "strange flight orbits" over Baltimore.⁶ These planes, it would later be learned, were equipped with powerful cameras capturing detailed imagery of the city from above. It was the latest evolution in the CitiWatch program—one that would afford the Baltimore Police Department unprecedented surveillance capabilities. Armed with both ground and aerial cameras, analysts could now identify potential suspects and track their movements across the city with precision.⁷ The planes, which flew for up to ten hours a day, were used by police to investigate everything from property thefts and shootings to unlicensed dirt-bikers.⁸ The public was told none of this.

4. See LA VIGNE ET AL., *supra* note 2, at 23–25.

5. See Marshall Greenlaw, *Baltimore Protests and Riots, 2015*, BLACKPAST (Dec. 17, 2017), <https://www.blackpast.org/african-american-history/baltimore-protests-and-riots-2015-2>.

6. See Monte Reel, *Secret Cameras Record Baltimore's Every Move From Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), <https://www.bloomberg.com/features/2016-baltimore-secret-surveillance>.

7. See BARRY FRIEDMAN, FARHANG HEYDARI, EMMANUEL MAULEÓN & MAX ISAACS, CIVIL RIGHTS AND CIVIL LIBERTIES AUDIT OF BALTIMORE'S AERIAL INVESTIGATION RESEARCH (AIR) PROGRAM 1–2 (2020), [https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5fc290577acac6192a142d61/1606586458141/AIR+Program+Audit+Report+vFINAL+\(reduced\).pdf](https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5fc290577acac6192a142d61/1606586458141/AIR+Program+Audit+Report+vFINAL+(reduced).pdf).

8. See Reel, *supra* note 6.

The existence of the spy planes became public in August 2016, when journalists published an exposé.⁹ Outrage ensued. The American Civil Liberties Union (ACLU) quickly issued a press release assailing the program as “a privacy nightmare come to life.”¹⁰ Congressman Elijah Cummings pledged to review the program and described its secret nature as “concerning.”¹¹ Said one city councilman, more bluntly: “The [police] commissioner keeps talking about transparency, but every time we turn around, there’s something else where we’re left on the outside.”¹² For its part, the Baltimore Police Department claimed that they did not disclose the aerial surveillance because it was merely an extension of the existing CitiWatch program.¹³ The flights soon were scuttled, but not before a public castigation of the Baltimore Police Department that further alienated it from the community it was sworn to protect.

Baltimore residents were the latest victims of function creep in policing technology. Without any laws on the books to prevent this expanded use of CitiWatch—or even provide the public with basic transparency around this use—legislators were left playing catch up to address violations of their constituents’ civil rights and liberties.

That policymaking is failing to keep pace with advances in surveillance technology has achieved the status of cliché. New innovations proliferate at a dizzying rate, rendering existing safeguards ineffective. Laws regulating these new products are few and far between—unsurprising because lawmakers themselves often lack the most basic information about the technologies that police use. This regulatory gap invites a race to the bottom among vendors

9. *See id.*

10. *See Police Secretly Put Large Part of Baltimore Under Constant Aerial Video Surveillance*, ACLU (Aug. 24, 2016), <https://www.aclu.org/press-releases/police-secretly-put-large-part-baltimore-under-constant-aerial-video-surveillance>.

11. *See* Luke Broadwater & Doug Donovan, *Baltimore City Council Plans Hearing on Undisclosed Police Surveillance Plane Program*, BALT. SUN (Aug. 25, 2016), <https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-surveillance-folo-20160825-story.html> [<https://web.archive.org/web/20210705134719/https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-surveillance-folo-20160825-story.html>].

12. *See* Luke Broadwater & Doug Donovan, *Baltimore City Council Plans Hearing on Undisclosed Police Surveillance Plane Program*, THE BALT. SUN (Aug. 25, 2016), <https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-surveillance-folo-20160825-story.html>.

13. *See* Brandon Soderberg, *Persistent Transparency: Baltimore Surveillance Plane Documents Reveal Ignored Pleas to Go Public, Who Knew About the Program, and Differing Opinions on Privacy*, BALT. SUN (Nov. 1, 2016), <https://www.baltimoresun.com/citypaper/bcp-110216-mobs-aerial-surveillance-20161101-story.html> [<https://web.archive.org/web/20210824223340/https://www.baltimoresun.com/citypaper/bcp-110216-mobs-aerial-surveillance-20161101-story.html>].

who manufacture and sell new and ever more intrusive surveillance tools to willing policing agencies, often with little proof of their benefits. When these programs inevitably come to light, they engender widespread outrage, distrust, and calls for accountability. Then the cycle begins anew.

As the Baltimore example illustrates, this system serves neither police nor the public well. “Hard law”—what we think of as law: statutes, regulations, and the like—is failing to keep the growth of surveillance and policing technologies in check.

In response to this logjam, the authors—lawyers at the Policing Project, a non-profit center at New York University School of Law—began a project to explore a “soft law” alternative: a certification system for policing technologies. The Policing Project is dedicated to making policing more transparent, equitable, and democratically accountable. Concerned by the unregulated use of technology by policing agencies, we sought and obtained a grant from the Alfred P. Sloan Foundation to study the value in a certification scheme for policing technologies. We studied the matter for the better part of a year, reading all the literature we could lay hands on and consulting numerous experts. Then we vetted the idea by convening relevant experts and stakeholders. All told, we spoke with over 50 people for our research, with equal participation from civil society, government, and industry.

A certification is a type of trademark that tells consumers that a product has met a particular standard. This form of “soft law” governance leverages market forces to promote a particular goal that is traditionally ignored or undervalued in the marketplace.¹⁴ Certification schemes are ubiquitous—if you’ve ever watched a “Rated R” movie, bought “Fair Trade” coffee, or purchased an “Energy Star” appliance, you’ve seen certification in action.

Our idea was that a certification scheme could perform a review of a technology’s efficacy and an ethical evaluation of its impact on civil rights, civil liberties, and racial justice. This, we surmised, would provide vital insights to policymakers and the public and perhaps even motivate the enactment of “hard law” (that is, statutes and regulations). Moreover, certification could create a market for policing products that are more protective of civil rights and civil liberties. And certification might address how products are actually *used* on the ground—Baltimore’s CitiWatch cameras, for example, might be

14. See POOJA SETH PARIKH, ENV’L L. INST., HARNESSING CONSUMER POWER 1 (2003), <https://www.eli.org/sites/default/files/eli-pubs/d13-05a.pdf>.

certified for use as traditional CCTV devices but not as part of an aerial surveillance system.¹⁵

Of course, certification is not without its normative challenges. Certification systems raise concerns about democratic legitimacy—most standard-setters and certifiers either are several steps removed from direct democratic processes or are entirely separate from them. Convincing policing agencies and technology vendors to adopt a certification scheme would be no small feat, and the threat of industry capture is an ever-present concern.

These points are well-taken but not insurmountable. As our Report explains, careful design and a set of institutional safeguards can help to ensure that certification is independent, responsive to public concerns, and valuable to lawmakers, vendors, and police alike. Whether a certification regime would accomplish all of this in practice is unclear. What *is* clear is that the status quo is unacceptable.

This Report proceeds in four Parts. In Part I, we survey the policing tech landscape and examine why policymakers largely have failed to regulate police use of emerging technologies. We then describe the result: a race to the ethical bottom in which any intrusive technological tool that can be dreamt up is sold to policing agencies and put into effect with little or nothing in the way of controls. In Part II, we propose certification for policing technologies as part of the solution. As we explain, certification might facilitate the enactment of hard law by addressing key challenges facing policymakers, including the lack of objective information and expertise about policing technologies. Moreover, certification could impose substantive ethical standards and create an incentive for vendors to compete along ethical lines. In Part III, we discuss a set of critical design choices for a policing certification scheme—how, for example, ought a certifier measure a product’s “benefits?” How could it account for the myriad ways that products might be used (or misused) in the real world? Finally, Part IV addresses some key challenges facing certification, including democratic legitimacy concerns, problems of compliance and enforcement, and the possibility that certification could function as a permission structure for agencies to acquire new technologies.

15. We recently applied a similar tool, an “audit,” to the latest iteration of Baltimore’s aerial surveillance program and found it severely wanting. See FRIEDMAN ET AL., *supra* note 7, at 3. Those planes no longer fly over Baltimore. See Mitchell Clark, *Baltimore’s Spy Planes Will Fly No More*, THE VERGE (Feb. 5, 2021), <https://www.theverge.com/2021/2/5/22267303/baltimore-maryland-shut-down-spy-plane-surveillance-program-vote>.

II. DEFINING THE PROBLEM

The use of emerging technologies by policing agencies is beset by two key problems.

The first problem can be thought of as structural: policymakers largely have abdicated their responsibility to regulate policing tech. A foundational principle of American governance is that executive agencies must be democratically accountable. That is, there must be rules—rules set ahead of time, with an opportunity for input from the public. If policing operated like other areas of government, legislators would put in place a means of assessing whether there is a policy framework under which use of a new technology can produce public safety benefits, while minimizing civil rights and civil liberties harms. Unfortunately, this sort of democratic accountability around policing technologies is all too rare.

The second problem is a consequence of the first: in the absence of regulation, tech vendors are enmeshed in a race to the ethical bottom, innovating new and ever more intrusive ways to track and surveil the citizenry. These technologies are marketed aggressively to policing agencies—often with completely unfounded claims about their public safety benefits. And agencies use these tools with little in the way of controls that mitigate their civil rights and civil liberties impact.

This Section proceeds in three parts. First, we survey the policing tech landscape—one defined by explosive change and a yawning information gap. Second, we explore the reasons why policymakers largely have failed to regulate police use of emerging technologies. And third, we describe the predictable result: a race to the bottom in which any intrusive technological tool that can be dreamt up is sold to policing agencies and put into effect with little or nothing in the way of controls.

A. THE POLICING TECH LANDSCAPE: WIDESPREAD USE, UNQUANTIFIED BENEFITS AND HARMS

Although early police in the United States had not much more than a nightstick at their disposal, many of today's agencies have a raft of sophisticated digital tools to choose from, ranging from aerial surveillance drones to biometric identification technologies to automated license plate readers, and much more.¹⁶ And they are putting these tools to use. Take, for

16. See generally Mathieu Deflem, *History of Technology in Policing*, in ENCYCLOPEDIA OF CRIMINOLOGY AND CRIMINAL JUSTICE 2269 (Gerben Bruinsma & David Weisburd eds., 2014).

example, face recognition technology (FRT). In 2016, a landmark report on law enforcement use of FRT estimated that one in four agencies have access to this tool, with over 117 million American adults already in face recognition databases.¹⁷ More recent investigative reporting revealed that nearly 7,000 public agency officials used FRT provided by Clearview AI—a company that scrapes billions of images from the internet without permission—often without any agency oversight.¹⁸

For many policing agencies, especially larger ones, face recognition is just the tip of the iceberg. In New York, the public learned for the first time (thanks to recently passed transparency legislation) that the New York Police Department (NYPD) has over 30 discrete surveillance tools at its disposal.¹⁹ The NYPD is by no means the only agency with access to these high-powered devices. Investigative reporting has revealed widespread use of surveillance technologies like cell-site simulators, mobile device forensic tools (MDFT), and automated license-plate readers (ALPRs) by thousands of agencies across the country. Over 2,000 agencies have purchased MDFTs, tools that enable police to download and programmatically search all data contained on a cellphone—from emails to texts to location data and more.²⁰ As far back as 2012, 71% of police departments were using ALPRs, resulting in scans of hundreds of millions of license plates.²¹ A 2020 California state auditor report

17. See GEORGETOWN L. CTR. ON PRIV. & TECH., *THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 1* (2016), <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf>.

18. See Ryan Mac, Carolina Haskins, Brianna Sacks & Logan McDonald, *Surveillance Nation*, BUZZFEED NEWS, <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition> (Apr. 9, 2021) [hereinafter Mac, *Surveillance Nation*].

19. See *Policies*, N.Y. POLICE DEP'T, <https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page> (last visited Mar. 31, 2022) (disclosing use and impact policies for over 30 surveillance technologies pursuant to the Public Oversight of Surveillance Technology Act, N.Y. CITY ADMIN. CODE § 14-188 (2020)); see also Ali Watkins, *How the N.Y.P.D Is Using Post-9/11 Tools on Everyday New Yorkers*, N.Y. TIMES (Oct. 13, 2021), <https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html> (reporting that the scope of N.Y.P.D's "surveillance dragnet" became clear "[o]nly recently" due to passage of transparency-forcing legislation).

20. LOGAN KOEPKE, EMMA WEIL, URMILA JANARDAN, TINUOLA DADA & HARLAN YU, UPTURN, *MASS EXTRACTION: THE WIDESPREAD POWER OF U.S. LAW ENFORCEMENT TO SEARCH MOBILE PHONES 4* (2020), <https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf>.

21. See AXON AI & POLICING TECH. ETHICS BD., *2D REPORT: AUTOMATED LICENSE PLATE READERS 13* (2019), <https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5dadec937f5c1a2b9d698ba9/1571679380452/>

revealed that the Los Angeles Police Department alone had stored more than 320 million license plate scans—99.9% of which were stored despite *not* generating a hot list match.²² Initially introduced in the 1990s to locate stolen vehicles, agencies now use ALPRs to conduct automated checks for unpaid parking tickets or inclusion in a gang database.²³ And thanks to improved data storage capabilities, these scans, which include time and location information, typically are stored and retained, creating massive databases that can track people’s movements over time.²⁴

In short, law enforcement use of technologies with super-charged abilities to collect information and conduct surveillance is widespread.

The widespread use of surveillance technologies by law enforcement might not be so concerning if the evidence were unequivocal that these tools made us safer and if communities were making informed choices to authorize the use of these tools, well aware of the potential harms. Unfortunately, neither of these things is true. Agencies deploy surveillance technologies with little information about effectiveness.²⁵ Undoubtedly some technologies have some benefits (while some may have little benefit at all), but there is almost no study of this issue. And what there is suggests the public safety benefits of even prominent technologies may be negligible.²⁶ The public and lawmakers often

Axon_Ethics_Report_2_v2.pdf; Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. (Sept. 10, 2020), <https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations>.

22. CAL. STATE AUDITOR, AUTOMATED LICENSE PLATE READERS 1 (2020), <http://auditor.ca.gov/pdfs/reports/2019-118.pdf>.

23. See AXON AI & POLICING TECH. ETHICS BD., *supra* note 21, at 13 (tracing the origins of police use of license plate readers to combatting auto theft); Díaz & Levinson-Waldman, *supra* note 21 (reporting on police use of license plate readers to create databases that can search for individuals with unpaid parking tickets or purported gang affiliations).

24. AXON AI & POLICING TECH. ETHICS BD., *supra* note 21, at 24–25.

25. See Cynthia Lum, Christopher S. Kroper & James Willis, *Understanding the Limits of Technology’s Impact on Police Effectiveness*, 20 POLICE Q. 135, 136–37 (2016); see also KEVIB STROM, OFF. OF JUST. PROGRAMS, RESEARCH ON THE IMPACT OF TECHNOLOGY ON POLICING STRATEGY IN THE 21ST CENTURY, FINAL REPORT (2016), <https://www.ojp.gov/pdffiles1/nij/grants/251140.pdf> (citing a body of research finding that agencies “select, implement, and integrate technology independent of existing empirical evidence or support for how these systems affect departmental operations, strategic decisions, or crime outcomes”).

26. STROM, *supra* note 25, at 4-4 (observing that “despite dramatic advances in DNA technology and computer databases for handling forensic data, clearance rates for violent and property crime have remained relatively stable since the mid-1990s” and citing studies); see also Lum et al., *supra* note 25 (generally reviewing the issue).

lack basic information and data about agency acquisition and use, rendering farcical any notion of democratic oversight.²⁷

The harms that flow from use of these technologies likewise are difficult to quantify, but there is still compelling evidence of their impact. Scholars have explained at length the theoretical and normative bases for how state surveillance chills the exercise of civil liberties and grants undue power to state actors.²⁸ Empirical research and historical experience has borne out these effects.²⁹ Worse still, these civil libertarian harms do not fall evenly upon all members of society. First, throughout American history surveillance technologies in the hands of the state have been deployed disproportionately on marginalized communities, especially Black communities.³⁰ From the FBI's COINTELPRO program to current day examples of police monitoring of Black Lives Matter activists, there is a persistent inclination of law enforcement to surveil minority communities.³¹ Second, these tools repeatedly have been used on those seeking social change by exercising First Amendment liberties.³²

27. See Mac, *Surveillance Nation*, *supra* note 18; Mihir Zaveri, N.Y.P.D. *Robot Dog's Run Is Cut Short After Fierce Backlash*, N.Y. TIMES (Apr. 28, 2021), <https://www.nytimes.com/2021/04/28/nyregion/nypd-robot-dog-backlash.html>; Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. (forthcoming 2022).

28. E.g., Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935; see also Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, 102 B.U. L. REV. (forthcoming 2022), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2790&context=faculty_publications (explaining a taxonomy of privacy harms).

29. Richards, *supra* note 28, at 1948 (“Our cultural intuitions about the [chilling] effects of surveillance are supported by . . . the empirical work of scholars in the interdisciplinary field of surveillance studies.”); Karen Gullo, *Surveillance Chills Speech—As New Studies Show—And Free Association Suffers*, ELEC. FRONTIER FOUND. (May 19, 2016), <https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association> (citing studies showing that government surveillance discourages speech and access to information on the Internet).

30. See generally SIMONE BROWN, DARK MATTERS: ON SURVEILLANCE OF BLACKNESS (2015); BARTON GELLMAN & SAM ADLER-BELL, THE CENTURY FOUND., THE DISPARATE IMPACT OF SURVEILLANCE (2017), <https://production-tcf.imgix.net/app/uploads/2017/12/03151009/the-disparate-impact-of-surveillance.pdf>.

31. MUDASSAR TOPPA & PRINCESS MASILUNGAN, STRUGGLE FOR POWER: THE ONGOING PERSECUTION OF BLACK MOVEMENT BY THE U.S. GOVERNMENT 1 (2021), <https://m4bl.org/wp-content/uploads/2021/08/Struggle-For-Power-The-Ongoing-Persecution-of-Black-Movement-by-the-U.S.-Government.pdf>. COINTELPRO was a covert federal surveillance program run by the FBI during the Cold War that targeted civil rights leaders and other political dissidents. See *More About FBI Spying*, AM. C.L. UNION, <https://www.aclu.org/other/more-about-fbi-spying> (last visited Mar. 31, 2022).

32. See e.g., Joanne Cavanaugh Simpson & Marc Freeman, *South Florida Police Quietly Ran Facial Recognition Scans to Identify Peaceful Protestors*, SUN SENTINEL (June 26, 2021), <https://>

There already are too many examples of the newer technologies—from face recognition to social media monitoring to aerial drones—being used to surveil lawful protestors speaking up against racial injustice.³³

More concretely, the harms that flow from these technologies also include false arrests and other wrongful enforcement actions. For example, law enforcement use of face recognition has led to three publicly known false arrests, all of Black men. Erroneous ALPR reads have led to faultless drivers being stopped and subjected to search and arrest. In Colorado, police detained, handcuffed and arrested a Black mother and her children after an ALPR scan incorrectly identified her car as stolen.³⁴ The chair of the Oakland Privacy Advisory Commission was stopped and held at gunpoint after a spurious ALPR scan.³⁵ These are but a few examples, but they are representative of the risks inherent in police use of these technologies. Yet, our ability to catalogue and quantify the scope and extent of technology-induced or enabled wrongful enforcement actions precisely is limited by the lack of basic information and transparency around law enforcement use of these tools.³⁶

In sum, the policing tech landscape can be defined by a massive information gap, which leaves us all in the dark regarding the benefits and harms and hinders democratic oversight—which we turn to next.

www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sl15uuaqfbeba32rndlv3xwxi-htmlstory.html; Sam Biddle, *U.S. Marshals Used Drones to Spy on Black Lives Matter Protests in Washington D.C.*, THE INTERCEPT (Apr. 22, 2021), <https://theintercept.com/2021/04/22/drones-black-lives-matter-protests-marshals/>.

33. See Allie Funk, *How Domestic Spying Tools Undermine Racial Justice Protests*, FREEDOM HOUSE (June 22, 2020), <https://freedomhouse.org/article/how-domestic-spying-tools-undermine-racial-justice-protests>.

34. Jessica Porter, *Aurora Police Detain Black Family After Mistaking Their Vehicle as Stolen*, THE DENVER CHANNEL (Aug. 3, 2020), <https://www.thedenverchannel.com/news/local-news/aurora-police-detain-black-family-after-mistaking-their-vehicle-as-stolen>.

35. See Lisa Fernandez, *Privacy Advocate Sues CoCo Sheriff's Deputies After License Plate Readers Target His Car Stolen*, KTVU FOX 2 (Feb. 19, 2019), <https://www.ktvu.com/news/privacy-advocate-sues-coco-sheriffs-deputies-after-license-plate-readers-target-his-car-stolen>.

36. See Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> (reporting Clare Garvie's comment in response to false arrest from FRT identification: "I strongly suspect this is not the first case to misidentify someone to arrest them for a crime they didn't commit. This is just the first time we know about it.").

B. THE ACCOUNTABILITY GAP

As a democratic society, we typically turn to legislation, regulation, and/or judicial review to address the types of harmful effects described above.³⁷ All of these measures are examples of “hard law” solutions, i.e., governance mechanisms with the force of law.³⁸ Yet, these measures have been few and far between. And hard law—standing alone—inevitably falls short in addressing the challenges presented by emerging police technologies.

1. *The current hard law landscape*

This Section provides a brief overview of current hard law oversight of policing technology and its limitations.

a) The limited constraints of constitutional judicial review

The Fourth Amendment—implemented by judges—is the primary constitutional restraint on police power, but under existing doctrine, remarkably few of the emerging police technologies fall within its ambit.³⁹ Under current law, individual conduct that takes place in public, or information given to third parties, is unprotected.⁴⁰ Even when the Fourth Amendment applies, the traditional tools of warrants and probable cause are of little help when mass data collection (such as is the case with automated license plate readers) is occurring. Similarly, when it comes to racial justice concerns, current equal protection jurisprudence fails to offer meaningful recourse, as it has been interpreted to prohibit only intentional discrimination by government agencies and officers; policies and practices that have a

37. See, e.g., Gary Marchant, Lucille Tournas & Carlos Ignacio Gutierrez, *Governing Emerging Technologies Through Soft Law: Lessons for Artificial Intelligence*, 61 JURIMETRICS J. 1, 4 (2020).

38. See *id.* at 4, 7 (comparing hard law solutions to soft law solutions).

39. See Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 838 (2004) (“Most existing Fourth Amendment rules in new technologies are based heavily on property law concepts, and as a result offer only relatively modest privacy protection in new technologies. . . . The key implication . . . is that we should not expect the Fourth Amendment alone to provide adequate protections against invasions of privacy made possible by law enforcement use of new technologies.”); see also Andrew Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1107–08 (2021) (“[D]esigned to restrain police power and enacted to limit governmental overreach . . . current [Fourth Amendment] doctrine and constitutional theory offer little privacy protection and less practical security than one might expect.”).

40. BARRY FRIEDMAN, HOOVER INST., PRIVATE DATA/PUBLIC REGULATION 6 (2021), <https://www.hoover.org/research/private-datapublic-regulation>.

disparate racial impact largely get a free pass in the courts.⁴¹ As Rachel Harmon summarizes it, “the public policy problems presented by the use of police power necessarily extend beyond constitutional law and the courts.”⁴²

b) Current legislative approaches: few and far between

The poor fit of constitutional review is especially concerning because it has served as our primary method of addressing policing, with legislation and administrative regulation historically taking a back seat.⁴³ At the federal level, legislation addressing policing is sparse. There is some regulation of police use of technology, such as the Electronic Communications Privacy Act, which includes provisions regulating government use of wiretaps.⁴⁴ There are also some federal laws that may regulate federal law enforcement’s collection and storage of personal data from biometric tools, such as the Privacy Act of 1974 and the E-Government Act of 2002.⁴⁵ In general, though, as many scholars have observed, “federal legislation [regulating policing] is limited in scope and often badly out of date.”⁴⁶

Regarding the tech companies, Congress “so far has done next to nothing to regulate them.”⁴⁷ There is some indication that the tide may be turning on

41. See e.g., Alexis Karteron, *Congress Can’t Do Much About Fixing Local Police—But it Can Tie Strings to Federal Grants*, THE CONVERSATION (June 1, 2021), <https://theconversation.com/congress-cant-do-much-about-fixing-local-police-but-it-can-tie-strings-to-federal-grants-159881>.

42. Rachel Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 763 (2012); see also Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 NYU L. REV. 1827, 1865 (2015) (“[F]or the most part, we look to the courts to tell police when they have overstepped their bounds. The difficulty is that . . . constitutional judicial review is completely inadequate for this task.”).

43. For an exposition of why policing agency regulation historically has been the province of judicial review, see generally Friedman & Ponomarenko, *supra* note 42.

⁴⁴18 U.S.C. §§ 2510–2522; see also CHARLES DOYLE, CONG. RSCH. SERV., R41733, *PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT* 24–28 (2012), <https://crsreports.congress.gov/product/pdf/R/R41733/9> (discussing applicability of ECPA provisions to government actors).

45. See KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, *FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT* 8–9 (2020), <https://crsreports.congress.gov/product/pdf/R/R46541> (discussing applicability of federal privacy legislation to face recognition technology).

46. Maria Ponomarenko, *Rethinking Police Rulemaking*, 114 N.W. L. REV. 1, 60 (2019) [hereinafter Ponomarenko, *Rethinking Police Rulemaking*].

47. Ed. Board, *Do Your Job and Regulate Tech, Congress—or States will Try to Do it for You*, WASH. POST (Feb. 19, 2021), https://www.washingtonpost.com/opinions/maryland-digital-ads-tax-regulate-tech/2021/02/19/368ab52c-721c-11eb-93be-c10813e358a2_story.html; Shira Ovide, *What Congress Wants from Big Tech*, N.Y. TIMES (June 24, 2021), <https://>

this account. For example, the Federal Trade Commission recently warned it would use its statutory grants of authority to regulate certain tech vendor practices, action which, if taken, could implicate some policing technologies.⁴⁸ Still, as it stands, unlike with cosmetics, medical devices, or products with environmental implications, there is no comprehensive federal legislative framework establishing rules and guidelines for policing technologies.

Although there is more legislative activity addressing policing technologies at the state and local levels, it still represents the exception more than the rule.⁴⁹ And it tends to focus on a single technology at a time. For example, 16 states have statutes addressing the use of ALPRs; fewer than a dozen states have passed legislation addressing law enforcement use of FRT.⁵⁰ This tech-by-tech statutory approach means “legislatures are delivering piecemeal rather than systemic, legislation” that is “tailored to the technology [du jour] rather than to the harm.”⁵¹ With new technology perpetually coming to market, a tech-by-tech statutory approach means legislators constantly are playing catch-up.

There also are some local jurisdictions that have passed information-forcing legislation, based on a model statute developed by the ACLU, Community Control Over Police Surveillance (CCOPS), that requires disclosure around law enforcement use of surveillance technologies. Despite its broader scope, this type of information-forcing legislation has struggled to make an impact. Since the ACLU launched its CCOPS legislative campaign in 2016, only 22 municipalities across the country have adopted this law. And several of these jurisdictions have seen agencies completely fail to comply with

www.nytimes.com/2021/06/24/technology/congress-big-tech.html (discussing recently proposed legislation to reign in big tech).

48. Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FED. TRADE COMM'N (Apr. 19, 2021), <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>.

49. Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 61 (“In policing . . . states do quite a bit more.”).

50. *E.g.*, AMBER WIDGERY, NAT'L CONF. STATE LEGISLATORS, LAW ENFORCEMENT USE OF TECHNOLOGY 16–17 (2021), <https://www.nmlegis.gov/handouts/CCJ%20072621%20Item%206%20Widgery%20Tech%20Slides%20final.pdf>. There also are a handful of states that regulate the collection of biometric information by private companies, protections which could apply to tech vendors that sell biometric tools to law enforcement. *See* Natalie Prescott, *The Anatomy of Biometrics Law: What U.S. Companies Need to Know in 2020*, THE NAT'L L. REV. (Jan. 15, 2020), <https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020>.

51. Maily Fidler, *Local Police Surveillance and the Administrative Fourth Amendment*, 36 SANTA CLARA HIGH TECH. L.J. 481, 544 (2020).

the statutory requirements.⁵² Others have seen agencies issue generic disclosures devoid of any meaningful information about use or impact. For example, in New York City, where the City Council passed a CCOPS-inspired statute, a coalition of 14 civil rights organizations and advocates, including the local chapter of the ACLU, found that the NYPD’s “boilerplate” responses were “plainly insufficient” and did not “reflect a good faith effort to comply” with statutory requirements.⁵³ In Oakland, the police department’s failure to comply with CCOPS legislation has led to a lawsuit from the chair of the Privacy Advisory Commission (PAC), the public body charged with oversight, who concluded that “the model is failing to work in Oakland and the other jurisdictions.”⁵⁴

c) Administrative body regulation: exceptions rather than rule

A handful of cities have turned to administrative agency solutions for oversight of policing technology acquisition and use—an approach that some policing scholars have touted as a particularly apt governance solution.⁵⁵ For example, Oakland’s PAC is an administrative body that, in conjunction with the City Council, oversees acquisition and use of any surveillance technologies used by law enforcement.⁵⁶ In addition, a number of major cities, including

52. *Community Control over Police Surveillance*, ACLU, <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance> (last visited Jan. 22, 2022); see, e.g., Ali Watkins, *How the N.Y.P.D. Is Using Post-9/11 Tools on Everyday New Yorkers*, N.Y. TIMES (Sept. 8, 2021) <https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html> (noting NYPD’s reluctance to fully comply with transparency requirements in POST Act, a watered-down version of CCOPS).

53. Letter from the N.Y. C.L. Union to Dermot Shea, Comm’r, N.Y.C. Police Dep’t (Feb. 24, 2021), https://www.nyclu.org/sites/default/files/field_documents/nyclu_letter_on_post_act_draft_policies_0.pdf; Letter from Civ. Soc’y to Dermot Shea, Comm’r, N.Y.C. Police Dep’t, & Margaret Garnett, Comm’r of the Dep’t of Investigation, Regarding the Public Oversight of Surveillance Technology Act (Feb. 24, 2021), <https://static1.squarespace.com/static/5c1bfc7ee175995a4ceb638/t/6036a7b9952aac14fd3df39d/1614194617915/POST+Act+Joint+Submission+%2802-24-21%29.pdf>.

54. Brian Hofer, *Why You Should Care About Our Lawsuit Against the City of Oakland*, SECURE JUST. (Sept. 2, 2021), <https://secure-justice.org/blog/why-should-you-care-about-our-lawsuit-against-the-city-of-oakland>.

55. See Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 1, 45–59 (arguing that we should consider creating “regulatory intermediaries” or permanent administrative bodies—such as inspectors generals or police commissions—that can stand in for the public to regulate the police); see also Fidler, *supra* note 51, at 481–82 (proposing that rather than legislate on these issues, city councils or a local appointed commission should be empowered to regulate the acquisition and deployment of police surveillance technologies).

56. Fidler, *supra* note 51, at 548–49; *Privacy Advisory Commission*, CITY OF OAKLAND, <https://www.oaklandca.gov/boards-commissions/privacy-advisory-board> (last visited Jan. 22, 2022).

Detroit, Los Angeles, San Francisco, and Chicago, have citizen-run police commissions that govern their police departments.⁵⁷ Regarding policing technologies specifically, several leading computer scientists recently have called for a new federal office—modeled on the Food and Drug Administration (FDA)—to regulate the use of face recognition technology by private and public actors, though nothing like this currently exists.⁵⁸ Still, despite these few promising examples and proposals, administrative agency bodies remain the exception not the rule for police technology oversight. And generalist commissions have done little to address technology issues.

2. *Obstacles facing hard law regulation of policing technology*

There are a set of obstacles that explain why the current regulatory landscape is sparse and inadequate. These obstacles set the stage for turning to certification as a possible partial solution:

a) Pacing Problem

Technological development today is happening “at an unprecedented pace,” which makes it “harder than ever to govern using traditional legal and regulatory means”—a phenomenon commonly referred to as the “pacing problem.”⁵⁹ Policing technology development is no exception. For example, in its evaluations of face recognition algorithms, the National Institute of Standards and Technology (NIST) reported “massive gains in accuracy” in the last five years, which “far exceeded” the improvements made in the preceding period.⁶⁰ Because government regulation is an inherently slow and bureaucratic process, it increasingly is difficult for it to keep up with these rapid

57. Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 47; Annie Sweeney, *Mayor Names Leader of New Civilian Commission Overseeing Chicago Police Department*, CHI. TRIB. (Jan. 10, 2022), <https://www.chicagotribune.com/news/criminal-justice/ct-civilian-police-oversight-head-20220110-so2f5xbra5ethppinotkjjfmhe-story.html>.

58. ERIK LEARNED-MILLER, VICENTE ORDÓÑEZ, JAMIE MORGENSTERN & JOY BUOLAMWINI, *FACIAL RECOGNITION TECHNOLOGIES IN THE WILD: A CALL FOR A FEDERAL OFFICE* (2020), https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRT'sFederalOfficeMay2020.pdf.

59. See Ryan Hagemann, Jennifer Huddleston Skees & Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 17 COLO. TECH. L.J. 37, 59 (2018); see also Adam Thierer, *The Pacing Problem, the Collingridge Dilemma & Technological Determinism*, TECH. LIBERATION FRONT (Aug. 16, 2018); Gary Marchant et al., *Addressing the Pacing Problem in THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT* 199 (2011).

60. Charles Romine, *Facial Recognition Technology (FRT)*, NAT'L INST. OF STANDARDS & TECH. (“NIST”) (Feb. 6, 2020), <https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0>.

developments in policing technologies.⁶¹ Perhaps worse, this rapid pace of development could mean that even if regulators could hurry to act, regulation “will likely be obsolete by the time the ink dries on the enactment.”⁶²

b) An Information Gap

This rapid pace of development and the inherent newness and uncertainty surrounding emerging technologies makes it difficult for policymakers to have the information required to support traditional regulation.⁶³ Put simply, new products enter the market ahead of scientific certainty about their benefits and harms, making it difficult, if not impossible, for regulators to have sufficient information with which to conduct an evaluation. Nor does there seem to be much effort to assess benefits and harms once these technologies are in use. With policing technologies, there also tend to be additional layers of obscurity around these products’ mere existence—often in the name of security—that inhibit legislative and regulatory oversight. For example, after the NYPD deployed a robotic surveillance dog without city council approval, councilmembers had to issue subpoenas to obtain basic details about its procurement.⁶⁴ A recent report issued by the U.S. Government Accountability Office (GAO) found that out of 14 federal law enforcement agencies that reported using external FRT systems, 13 had *no idea* which systems their personnel were using.⁶⁵ One agency initially informed the GAO that it did not use any external FRT systems but was forced to correct this representation after an internal poll showed that its employees had conducted over 1,000 face

61. See Gary E. Marchant, Douglas J. Sylvester & Kenneth W. Abbott, *A New Soft Law Approach to Nanotechnology Oversight: A Voluntary Product Certification Scheme*, 28 UCLA J. ENV'T L. & POL'Y 123, 130 (2010); Gary Marchant & Wendell Wallach, *Toward the Agile and Comprehensive International Governance of AI and Robotics*, 107 POINT OF VIEW 505, 505 (2019), <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=8662741> (“Rapidly emerging technologies . . . are advancing so quickly that in many sectors, traditional regulation cannot keep up, giving the cumbersome procedural and bureaucratic procedures and safeguards that modern legislative and rulemaking processes require.”); see also Hagemann et al., *supra* note 59, at 58–59, 61 (discussing “the accelerating pace of ‘the pacing problem’” and arguing that “[m]odern technological innovation is occurring at an unprecedented pace, making it harder than ever to govern using traditional legal and regulatory mechanisms”).

62. Marchant & Wallach, *supra* note 61.

63. Marchant et al., *supra* note 61, at 130.

64. See Zaveri, *supra* note 27.

65. U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-105309, FACIAL RECOGNITION TECHNOLOGY: FEDERAL LAW ENFORCEMENT AGENCIES SHOULD HAVE BETTER AWARENESS OF SYSTEMS USED BY EMPLOYEES 10 (2021), <https://www.gao.gov/assets/gao-21-105309.pdf>.

recognition searches on external systems.⁶⁶ Without basic information about which products agencies are even using, neither legislators nor the public can begin to evaluate these tools.

c) An Expertise Gap

Even when there is awareness and knowledge about law enforcement use of these technologies, policymakers often lack the expertise needed to adequately evaluate these increasingly complex tools.⁶⁷ In particular, new policing tools that incorporate machine learning (ML) technology can require advanced degrees in computer and data sciences to analyze their functions and limitations.⁶⁸ Legislators face an ever-steeper learning curve in the face of these new developments. Yet effective legislation and regulation requires a full understanding of how these technologies work and interact with each other, their capabilities, their flaws, and their impact on people. In our current system, it is difficult if not impossible for legislators and regulators to acquire this level of understanding.

d) A Public Choice Problem

In the absence of digestible information about the risks these technologies pose, anti-regulatory pressures from interest groups like police unions and other law enforcement organizations dominate.⁶⁹ Even in the wake of widespread calls for police reform, being labeled “soft on crime” remains a political death knell.⁷⁰ Consider the collapse of bipartisan negotiations around federal police reform legislation because of an inability to reach consensus

66. *Id.* at 11.

67. Timothy Lytton, *Competitive Third-Party Regulation: How Private Certification Can Overcome Constraints That Frustrate Government Regulation*, 15 THEORETICAL INQUIRIES L. 539, 543 (2013) (explaining how “limited expertise” can frustrate government efforts to regulate); Hagemann et al., *supra* note 59, at 69 (discussing the “knowledge problem” regulators face when it comes to emerging technologies and the lack of regulatory expertise); Fidler, *supra* note 51, at 530 (“Neither judges nor legislators nor municipal officials will be experts on investigative technology. . . . Administrative oversight does not solve this [expertise] problem.”); *see generally* Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46.

68. *See* Sebastian Klovig Skelton, *UK Regulators Lack The Skills and Expertise to Cope with Increasing Use of Algorithms*, COMPUTERWEEKLY.COM (Oct. 15, 2020), <https://www.computerweekly.com/news/252490597/UK-regulators-lack-the-skills-and-expertise-to-cope-with-increasing-use-of-algorithms>.

69. Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 62 (“Police unions and other law enforcement organizations are a powerful force in state-level politics.”).

70. Friedman & Ponomarenko, *supra* note 42, at 1863–64 (discussing legislative inaction on policing and observing that “[t]here are few labels in American politics more damning than ‘soft on crime.’ For the most part, then, legislatures are content to leave well enough alone.”).

around qualified immunity, a deal breaker for police unions.⁷¹ As public choice theory would predict, legislators are reticent to step into the fray of contentious issues for fear of offending powerful interest groups or large segments of their voters and thereby hurting their chances of reelection.⁷²

Policymakers also face anti-legislative pressures from industry, particularly in light of the competitive national and international marketplaces. As in the tech industry writ large, policing technology vendors employ powerful lobbying groups across Washington and statehouses. Many vendors operate across state or national borders, creating downward pressure on both local and national governments to impose restrictive regulations that could impede their competitiveness in the broader marketplace.⁷³

e) Federalist Fragmentation

Pace aside, state and local hard law solutions for policing technologies also present problems of fragmentation. By and large, these technology products are not designed for a particular agency or deployed in a single jurisdiction. They mostly are off-the-shelf tools that raise similar concerns wherever they are deployed. Relying on local legislation or regulation as a solution means expecting each jurisdiction to develop its own evaluative matrix for these complex tools. Take the example of a face recognition algorithm that research has shown can produce racially biased results. How is an ordinary lay entity expected to vet this claim? By reviewing the black box of machine learning code to see if a particular system exhibits this bias? Such a localized analysis

71. Jacob Pramuk, *Police Reform Talks Fall Apart after Months of Bipartisan Negotiations in Congress*, CNBC (Sept. 22, 2021), <https://www.cnbc.com/2021/09/22/police-reform-booker-bass-scott-negotiations-fall-apart.html>; see also Fidler, *supra* note 51, at 542–43 (“[C]ongressional interest has waned for [many policing] technologies. . . . Little federal Congressional action on related [issues] has happened since the early 2000s.”).

72. See Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice*, 44 SYRACUSE L. REV. 1079, 1086–92 (1993) (detailing the relationship between voters, legislators, and criminal procedure decisions); Ronald Wright, *Parity of Resources for Defense Counsel and the Reach of Public Choice Theory*, 90 IOWA L. REV. 219, 257–58 (2004) (discussing legislatures’ willingness to approve and fund, rather than restrict, police activity because benefits are generalized while surveillance harms disproportionately affect already marginalized groups); cf. Rachel Barkow, *Federalism and the Politics of Sentencing*, 105 COLUM. L. REV. 1276, 1278–83 (2005) (describing the public choice problem in sentencing law).

73. Hagemann et al., *supra* note 59, at 71–74; see also GARY MARCHANT, AI PULSE, SOFT LAW GOVERNANCE OF ARTIFICIAL INTELLIGENCE 3 (2019), <https://aipulse.org/soft-law-governance-of-artificial-intelligence/?pdf=132> (discussing regulation of emerging AI technologies and concluding that “national governments are reluctant to impede innovation in an emerging technology by preemptory regulation in an era of intense international competition”).

would be inefficient, unrealistic, and risk the creation of inconsistent and conflicting conclusions across jurisdictions.⁷⁴ Although federal legislation might avoid this fragmentation problem, it still would have to wrestle with federalism constraints when it comes to oversight of local policing.⁷⁵

C. THE RESULTANT RACE TO THE BOTTOM

In the absence of adequate legislation and regulation, market forces hold sway, creating a race to the bottom in which any intrusive technological tool that can be dreamt up is sold to policing agencies and put into effect with little or nothing in the way of controls. Policing agencies, which consider it their mission to keep the public safe, seek and purchase products that they are told by vendors promise the greatest security benefits. Producers of these technologies innovate to meet this demand, focusing on tools that assist agencies in gathering information about and from the public, while paying little attention to ethical implications.⁷⁶ Although the public and elected officials have an interest in protecting civil rights and liberties, their ability to surface their demand for these criteria is stymied by the information, expertise, and public choice problems described above.⁷⁷ Simply put, when it comes to policing technologies, we have a race to the ethical bottom.

74. See, e.g., Ponomarenko, *Rethinking Police Rulemaking*, *supra* note 46, at 45 (discussing local administrative regulatory bodies for police oversight, with over 18,000 agencies, “these sorts of regulatory structures may not be a viable solution to the problems of policing writ large”).

75. Fidler, *supra* note 51, at 541–42 (“[P]artway is the furthest we’d get with a top-down federal approach.”).

76. See David Priest, *Ring’s police problem never went away. Here’s what you still need to know*, CNET (Sept. 27, 2021), <https://www.cnet.com/home/security/rings-police-problem-didnt-go-away-it-just-got-more-transparent/>; April Glaser, *How to Not Build a Panopticon*, SLATE (July 19, 2019), <https://slate.com/technology/2019/07/amazon-rekognition-surveillance-panopticon.html> (reporting on the successful expansion of Amazon’s Ring product without consideration for its civil liberties concerns); Priyanka Boghani, *Amazon Exec Defends Recognition Sales to Law Enforcement, Says Would Sell to Foreign Governments*, PBS FRONTLINE (Feb. 8, 2020), <https://www.pbs.org/wgbh/frontline/article/amazon-aws-ceo-andy-jassy-defends-facial-recognition-sales-law-enforcement-says-would-sell-to-foreign-governments> (describing Amazon’s push to sell facial recognition technology to law enforcement despite concerns raised by civil rights groups); see also Elizabeth Joh, *The Undue Influence of Surveillance Companies on Policing*, 92 N.Y.U. L. REV. 19, 20–21 (2017) (observing that despite surveillance technology vendors’ significant influence over police, vendors largely are not publicly accountable for their products’ impacts on civil liberties).

77. See Kira Matus, *Standardization, Certification, and Labeling: A Background Paper for the Roundtable on Sustainability Workshop January 19–21, 2009*, in CERTIFIABLY SUSTAINABLE? THE ROLE OF THIRD-PARTY CERTIFICATION SYSTEMS: REPORT OF A WORKSHOP 79, 83–84 (2010), <https://www.nap.edu/read/12805/chapter/12> (discussing how certification can be a

But the fact that the hard law governance landscape currently is insufficient is neither surprising nor cause to lose hope for effective oversight of policing technologies. Many of the regulatory challenges described above are common across sectors dealing with emerging technologies from the financial industry to biomedicine.⁷⁸ Rather, it is reason to explore whether there are other approaches that may help remove some of the obstacles facing legislative and regulatory approaches or fill in the regulatory void, at least in part. As Gary Marchant has explained, emerging technology governance is a “wicked problem” for which “there will not be a single, effective solution . . . [r]ather, the best strategy will be to integrate a number of imperfect tools, recognizing and trying to compensate for their particular flaws.”⁷⁹

In the remainder of this Report, we explore whether a “soft law” tool, namely a product certification system, might have a role to play in solving the “wicked problem” of emerging policing technology governance.

III. PRODUCT CERTIFICATION AS PART OF THE SOLUTION?

A. WHAT WE’RE EXPLORING

So far, we’ve seen two general problems: there is not enough hard law to regulate policing technologies because of a set of factors—pacing, lack of information, lack of expertise, political self-interest, and the regulatory fragmentation of our federal system; and there is a resultant race to the bottom. Here, we explore the idea of certification as a partial solution to these problems. Certification systems “attempt[] to harness market forces” to promote a particular goal or set of goals that currently are ignored or undervalued in the marketplace.⁸⁰ They are a form of “soft law”—or “program[s] that create[] substantive expectations, but which are not directly

useful regulatory solution for products with impacts that may evade typical marketplace incentives).

78. Hagemann et al., *supra* note 59, at 41; *see also* GARY MARCHANT, *EMERGING TECHNOLOGIES: ETHICS, LAW, AND GOVERNANCE* 1 (2017) (“One of the distinguishing features of most emerging technologies is that they present a broad range and diversity of ethical and social issues.”).

79. Gary Marchant, *Governance of Emerging Technologies as a Wicked Problem*, 73 *VAND. L. REV.* 1861, 1862–63 (2020).

80. POOJA SETH PARIKH, *ENV’L L. INST., HARNESSING CONSUMER POWER: USING CERTIFICATION SYSTEMS TO PROMOTE GOOD GOVERNANCE* 1 (2003), <https://www.eli.org/sites/default/files/eli-pubs/d13-05a.pdf>; *see also* Matus, *supra* note 76, at 83–84 (explaining that certification allows consumers “to have more information regarding impacts of their consumption that would otherwise be unobservable to them”).

enforceable by government.”⁸¹ Certification systems both provide an additional level of regulation, albeit without the formal enforcement of hard law, and they can provide some of the information and expertise that is needed to break the public choice logjam and enable hard law itself.

The basic concept we have been studying is a product certification system in which producers of policing technologies would submit their products for evaluation. The evaluation would involve two functions. First, it would perform some sort of *efficacy review*. At minimum, this would entail evaluating whether/how well the product does what it purports to do. Or it could go further and conduct a more holistic assessment of whether there is clear evidence for the notion that its use would enhance public safety. Second, products would undergo an *ethical review*, which would entail assessing the product along a list of dimensions including privacy, racial justice, data protection, and the like. We explore certification design in-depth in Part III. But first, some examples.

B. COMMON CERTIFICATION EXAMPLES

Product certification is not a new concept. It currently is used in varying forms across disparate industries. Common examples include:

Table 1: Examples of Certification Schemes

B Lab Certification	B Corporations are for-profit businesses that meet certain standards of “social and environmental performance,” as certified (for a fee) by the nonprofit organization B Lab. Its certification standards assess whether the corporations create value for non-shareholding stakeholders, including their employees, community members, customers, and the environment, as determined via ~200 question “Impact Assessment.” Companies also must satisfy certain legal requirements. B Lab publishes a final Impact Report, which contains a summary of a company’s Impact Assessment scores.
USDA “Organic” Certification	The U.S. Department of Agriculture (USDA) accredits state or private agencies to certify food products or farms that adopt practices that comply with the USDA’s organic regulations. Entities submit an application (with fees) to a USDA-accredited certifier, which includes a “detailed description of the operation to be certified” and a written plan “describing the practices and substances to be used.” Certifiers review the written application, and if approved, an

⁸¹. Marchant et al., *supra* note 37, at 5.

	inspector visits the operation to verify compliance. An approved entity receives an organic certificate which allows it to sell, label, or represent its products as “organic.” The USDA website maintains a database of certified organic farms and businesses with basic information about what’s been certified.
Gem Certification	The Gemological Institute of America (GIA) issues a “Diamond Grading Report” which provides information on various diamond features, including shape, clarity, cut, and carat weight. Jewelers voluntarily submit a gem for review and receive a detailed report describing the gem across these various categories. These reports often are provided to prospective purchasers. Although the GIA reports provide categorical grades, they do not make ultimate purchasing recommendations.

C. CERTIFICATION FOR POLICING TECHNOLOGY: ABSENCE AND DEMAND

Certification entities like those just described do not exist, nor have they ever, for policing technologies. Yet there presently are some proposals and programs that would require the existence of, or indicate buy-in for, certification in the policing tech space.

The European Commission’s recently proposed Artificial Intelligence Act would require high-risk AI systems used by law enforcement, such as face recognition technology, to undergo an independent pre-market certification process to assess compliance with EU specifications. These include requirements for data governance, system transparency, human oversight, accuracy, robustness, cybersecurity, and auditability.⁸² To retain their certification, these systems also will be subject to post-market surveillance and supervision.⁸³ Thus, tech vendors looking to sell their AI systems to law enforcement in Europe soon may be subject to a certification process with ethical components.

82. Eve Gaumont, *Artificial Intelligence Act: What is the European Approach for AI?*, LAWFARE (June 4, 2021), <https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai>.

83. THEODORE CHRISTAKIS, MATHIAS BECUYWE & AI-REGULATION TEAM, FACIAL RECOGNITION IN THE DRAFT EUROPEAN AI REGULATION: FINAL REPORT ON THE HIGH-LEVEL WORKSHOP HELD ON APRIL 26, 2021 (2021), <https://ai-regulation.com/wp-content/uploads/2021/05/Final-Report-26-04.pdf>.

Although there is no official U.S. government parallel to the European Commission's certification proposal, a recent report issued by the Federation of American Scientists (FAS) urges federal action to create a "Digital Surveillance Oversight Committee" (DSOC), a multi-stakeholder certification body, housed in a federal agency, that would certify current and emerging surveillance technologies used by public agencies—including local law enforcement—across ethical dimensions.⁸⁴

Several non-governmental organizations recently have piloted certification systems that would include *some* technology products used by law enforcement in their remit.⁸⁵ Most notably, in 2018, the Institute of Electric and Electronic Engineers (IEEE), the world's largest technical professional organization and a major player among standards-setting organizations, launched an "ethics certification program" for AI systems (ECPAIS) with the goal of developing a certification process that would address transparency, accountability, and reduction of algorithmic bias in AI systems.⁸⁶

Although not a certification system, NIST's ongoing series of Face Recognition Vendor Tests (FRVT) bears mentioning as well. For over a decade, NIST has conducted benchmark testing to measure face recognition systems' algorithmic accuracy.⁸⁷ These tests do not certify algorithmic compliance with a particular set of national standards nor does NIST place a "seal of approval" on any particular algorithm. But, in issuing public reports ripe with vendor-specific performance data and maintaining a dynamic "leaderboard" ranking algorithm performance on its website, its evaluations and rankings have become powerful motivators for industry improvement as evidenced by vendors' frequent citation to their NIST standings in press and

84. ISHAN SHARMA, FED'N OF AM. SCIENTISTS, A MORE RESPONSIBLE DIGITAL SURVEILLANCE FUTURE 32–34 (2021), <https://uploads.fas.org/2021/02/Digital-Surveillance-Future.pdf>.

85. E.g., *The Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)*, IEEE SA, <https://standards.ieee.org/industry-connections/ecpais.html>; SEBASTIEN LOURADOUR & LOFRED MADZOU, WORLD ECONOMIC FORUM, RESPONSIBLE LIMITS ON FACIAL RECOGNITION: USE CASE: FLOW MANAGEMENT PART II (2020), https://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf. See generally *Soft Law Governance of Artificial Intelligence*, CTR. FOR L., SCI. & INNOVATION, ASU SANDRA DAY O'CONNOR COLL. OF L., <https://lsi.asulaw.org/softlaw> (last visited Jan. 27, 2022) (presenting a database of over 600 soft law programs targeting AI technologies, including certification systems).

86. IEEE SA, *supra* note 85.

⁸⁷*About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 116–60 (2020) (statement of Charles H. Romine, Director of the Info. Tech. Lab'y, Nat'l Inst. Standards & Tech.).

sales materials.⁸⁸ As a result, what NIST measures can end up counting for a lot in shaping industry practice. For example, researchers have observed that NIST’s decision to evaluate demographic effects on accuracy has “ensur[ed] such concerns propagate into industry systems.”⁸⁹

The growing use of “ethics” or “advisory” boards by policing technology companies also is worth mentioning as it indicates an awareness on the part of tech companies that the status quo will not suffice. From 2019 to 2022, Axon, a major policing technology vendor, set up an AI Ethics Board made up of experts in the fields of AI, computer science, privacy, law enforcement, civil liberties, and public policy. The Board’s purpose was to guide the company “around ethical issues relating to the development and deployment of artificial intelligence (AI)-powered policing technologies.”⁹⁰ In response to the Board’s report highlighting the risks of FRT, for example, Axon agreed to not proceed with adding FRT capabilities to its body-worn cameras.⁹¹ And in a naked attempt to counter its invasive and potentially illegal practices, Clearview stood up an “independent” advisory board—staffed almost entirely with former law enforcement or national security officials—with a stated mission of ensuring

88. See, e.g., *FRVT 1: N Identification*, NAT’L INST. STANDARDS & TECH., <https://pages.nist.gov/frvt/html/frvt1N.html> (last visited Apr. 5, 2022) (linking to public report evaluating face recognition algorithms and displaying table ranking face recognition algorithm performance); *Idemia’s Facial Recognition Ranked #1 in NIST’s Latest FRVT Test*, IDEMIA (Apr. 6, 2021), <https://www.idemia.com/press-release/idemias-facial-recognition-ranked-1-nists-latest-frvt-test-2021-04-06> (citing performance on NIST testing in press release); *NEC Face Recognition Technology Ranks First in NIST Accuracy Testing*, NEC (Aug. 23, 2021), https://www.nec.com/en/press/202108/global_20210823_01.html (same); see also Samuel Dooley, Tom Goldstein & John P. Dickerson, *Robustness Disparities in Commercial Face Detection 1*, ARXIV:2108.12508 (Aug. 27, 2021), <https://arxiv.org/pdf/2108.12508.pdf> (discussing the role of NIST testing as a “guardrail that has spurred positive, though insufficient, improvements and widespread attention”).

89. Dooley et al., *supra* note 88.

90. *Axon AI Ethics Board*, POLICING PROJECT N.Y.U. SCH. OF L., <https://www.policingproject.org/axon-ethics-board> (last visited Jan. 27, 2022). In 2022, the AI Ethics Board disbanded following the resignation of nine Board members in response to Axon’s announcement that it was proceeding with development of TASER-equipped drones to be deployed in schools and other potential targets for mass shootings. See *Statement of Resigning Axon AI Ethics Board Members*, POLICING PROJECT (June 6, 2022), <https://www.policingproject.org/statement-of-resigning-axon-ai-ethics-board-members>. Axon has now announced that it is pausing work on the TASER drone project. See Rick Smith, *Axon Committed to Listening and Learning So That We Can Fulfill Our Mission to Protect Life, Together*, AXON (June 5, 2022), <https://www.axon.com/news/technology/axon-committed-to-listening-and-learning>.

91. Chaim Gartenberg, *Axon (formerly Taser) Says Facial Recognition on Police Body Cams is Unethical*, THE VERGE (June 27, 2019), www.theverge.com/2019/6/27/18761084/axon-taser-facial-recognition-ban-ethics-board-recommendation.

that its face recognition technology is “used . . . according to the highest professional standards to keep communities safe.”⁹² To date, Clearview’s Advisory Board has not taken any public action.

These proposed requirements, and emerging models, indicate that various experts and key stakeholders believe there is value to the use of some sort of certification regime to help address the governance gaps raised by policing agencies and governmental use of emerging technologies with the capacity for surveillance and information-collection.

D. CERTIFICATION AS AN ANSWER TO KEY POLICING TECHNOLOGY GOVERNANCE CHALLENGES

In theory, certification for policing technologies both could foster democratic accountability and mitigate the current race to the bottom.⁹³

1. *Supplying Information and Expertise to Foster Democratic Accountability*

A certification system for policing technologies could assist policymakers by addressing the information and expertise gaps that currently stymie effective hard law governance. By definition, certification communicates information about products.⁹⁴ Through highlighting which products policing agencies are using as well as the particular attributes and impact of these tools, certification could influence purchasing decisions by policing agencies and the jurisdictions they serve and aid regulators drafting legislation and rules. Certifiers also could require vendors to implement transparency-forcing mechanisms, such as transparency portals—online portals that could disclose information about how police use technology. In these ways, certification systems could help provide information the public and legislators currently lack—information that is essential to support traditional regulation.

92. *Clearview AI Announces Formation of Advisory Board*, BUSINESSWIRE (Aug. 28, 2021), <https://www.businesswire.com/news/home/20210818005288/en/Clearview-AI-Announces-Formation-of-Advisory-Board>.

93. See, e.g., Carlos Ignacio Gutierrez & Gary Marchant, *Soft Law 2.0: Incorporating Incentives and Implementation Mechanisms Into the Governance of Artificial Intelligence*, ORG. FOR ECON. CO-OPERATION & DEV. (July 13, 2021), <https://oecd.ai/en/wonk/soft-law-2-0> (observing that soft law mechanisms “can . . . serve as a precursor or as a complement or substitute to regulation”); Mallory Elise Flowers, Daniel C. Matisoff & Douglas S. Noonan, *In the LEED: Racing to the Top in Environmental Self-Regulation*, 29 BUS. STRATEGY & ENV’T 2842, 2843, 2852–53 (2020) (finding that a green building certification program created a “race to the top” in improving buildings’ environmental performance).

94. NAT’L RSCH. COUNCIL, *CERTIFIABLY SUSTAINABLE?: THE ROLE OF THIRD-PARTY CERTIFICATION SYSTEMS: REPORT OF A WORKSHOP 19* (2010), <https://www.nap.edu/read/12805/chapter/1>.

In addition, certification systems similarly can address the expertise gaps that often prevent effective regulation. Because they have fewer barriers to employing or contracting with a broad range of subject matter experts to review and evaluate products—certification systems can draw on, they are able to acquire technical expertise that policing agencies, legislatures, and regulatory bodies cannot access as easily.⁹⁵

2. *Evading Hard Law Challenges to Curb the Race to the Bottom*

As discussed, in the absence of regulation, we are living with a technological race to the bottom—a race which certification systems could disrupt through setting substantive ethical standards. By setting standards for ethical use, a successful certification regime can construct a raised floor and create an incentive for vendors to compete along ethical lines.

Although certification should not be seen as a *replacement* for regulation, setting substantive standards through certification both can serve some helpful function in the absence of regulation and also can shore up regulation where it exists because it avoids some of the key problems facing policymakers. First, because it is a non-legislative body (whether public or private) with a distinct mission, certification will not be burdened with the public choice problems that have thrown legislative bodies into stasis. Members of this body will have no reason to fear public opinion injuring their electoral chances. And constructed properly, they would be beholden to no particular entities or interest groups. (We address the issue of industry capture in Section III.E). In addition, certification can bring salience to problems around policing tech in a way that can break the regulatory logjam.

Second, because a certification system need not comply with a panoply of bureaucratic and procedural requirements, it can better keep pace with rapid technological changes, establish standards more quickly than some regulatory bodies, and revisit issues more frequently.⁹⁶ This flexibility would enable it to keep pace with rapid technological changes.⁹⁷ For example, the entity could re-evaluate a given vendor's face recognition software whenever there is a

95. Lytton, *supra* note 67, at 564; cf. Lesley K. McAllister, *Harnessing Private Regulation*, 3 MICH. J. ENV'L & ADMIN. L. 291, 294 (2014) (noting that a “[c]ommonly cited benefit[]” of non-governmental forms of regulation is “increasing expertise”); David M. Lawrence, *Private Exercise of Governmental Power*, 61 IND. L.J. 647, 656–57 (1985) (citing the “availability of special expertise” as an advantage of delegating regulation to private actors); NAT'L RSCH. COUNCIL, *supra* note 94, at 11; Hagemann et al., *supra* note 59, at 92 (observing that “[r]egulators . . . are increasingly reliant on the expertise housed in private firms to execute best practices and standards”).

96. *Id.*

97. See, e.g., Marchant et al., *supra* note 37, at 7.

significant software update or a new use case is discovered without having to wade through more rigid agency approval processes.

Finally, a the reach of a certification entity would not be subject to can evade issues of regulatory fragmentation because it could evaluate products and producers (and perhaps uses, more on that below) at one central node, providing useful information and expertise that the many individual local entities—from policing agencies to local and state legislatures—could piggyback upon. Local jurisdictions could rely on certification results for complex algorithms, rather than having to conduct their own evaluations from scratch, an impossible task for most jurisdictions.

E. THEORIES OF CHANGE

Having laid out how certification might address the key challenges to policing tech governance, we now turn to the underlying mechanism(s) that would allow a certification entity to produce these changes, i.e., the theory (or theories) of change that would guide development.

First, certification can effect change by incentivizing tech vendors to produce more ethical and transparent products. Vendors benefit if the system helps their bottom line and/or burnishes their brand. By providing clear ethical goals toward which companies can work and a label that signals compliance, certification can help companies differentiate themselves in the marketplace and protect their reputations, thereby ending the race to the ethical bottom that many vendors are engaged in at present. After all, reputation is a “fundamental organizational asset,” and certification would serve as a tool for companies to use in promoting their social responsibility.⁹⁸ (Vendors also might value certification if it helps ward off regulation, a challenge and concern we discuss in Section IV.D.)

Second, certification can effect change by influencing policing agencies to choose products that are more ethical. Policing agencies and the jurisdictions they serve would benefit from certification because it would enable agencies to choose technologies wisely and thus use them with less concern about public backlash. Relying on emerging technology in a non-transparent way has caused a great deal of suspicion in the general public. At times, law enforcement has been denied the ability to continue using those tools altogether. For example, the Seattle Police Department had to abandon its drone program, which included two helicopter drones acquired without

98. Carlos Ignacio Gutierrez, Gary Marchant & Lucille Tournas, *Lessons for Artificial Intelligence from Historical Uses of Soft Law Governance*, 61 JURIMETRICS J. 133, 140 (2020).

democratic approval or public awareness, after facing fierce public backlash.⁹⁹ Reacting to San Francisco's ban on FRT use by law enforcement, the head of the National Police Foundation conceded that "our traditional secrecy and lack of transparency has probably come back to haunt us."¹⁰⁰ In addition, policing officials complain that they are overrun with pitches from vendors and that it is difficult to distinguish one product from another. Certification could eliminate some of this uncertainty and provide a guide to products that meet some level of ethical standards, as well as those that (at least) perform as intended. Indeed, law enforcement we spoke with repeatedly emphasized the need for a source of objective, comparative information about how these tools operate.

Third, certification can effect change by helping legislators, the media, and the public better understand and compare the ethical implications of policing technologies. The public could benefit from certification in two main ways: (1) certification could raise the salience of emerging policing technologies and thus motivate hard law regulation, and/or (2) it could create a market for products that are more protective of civil rights and liberties thus reducing harm. As Part I made clear, dysfunction in the hard law system has led to adoption of potentially harmful technologies with almost no regulation. Members of the public and the media may not know about the technologies at all, and they have no way to evaluate their purported benefits or ethical impacts. Certification could serve as a tool to disseminate the information required to produce a more transparent marketplace and prompt a functional regulatory ecosystem.

Similarly, regulators suffer at present from a host of obstacles—from lack of information and expertise to pressures not to regulate the police and thus appear soft on crime. Certification would provide needed information, vetted by experts. Certification might help with the public choice logjam as well: if some products are certified as acceptable, and others not, regulators would have a roadmap of how to proceed to regulate in a way that could attract public acceptance. Certification gives them cover of a sort. (As noted above, though, certification may deter regulation, an issue we take up Section IV.D).

The extent to which each of these theories of change are distinct or overlapping is debatable. The bottom line is that for a policing technology

99. Christine Clarridge, *Seattle Grounds Police Drone Program*, SEATTLE TIMES (Feb. 7, 2013), <https://www.seattletimes.com/seattle-news/seattle-grounds-police-drone-program>.

100. Jon Schuppe, *San Francisco's Facial Recognition Ban is Just the Beginning of a National Battle Over the Technology*, NBC NEWS, <https://www.nbcnews.com/news/us-news/san-francisco-s-facial-recognition-ban-just-beginning-national-battle-n1007186> (May 22, 2019).

certification system to work, it must be valued by some combination of the key stakeholder groups in this ecosystem: law enforcement, policymakers, the public, and tech vendors.¹⁰¹

Of course, identifying a theory—or theories—of change does not guarantee that a particular intervention will achieve the desired outcome. Many questions around viability cannot be answered until a system actually is in place. But considering theory of change along with other substantive criteria does provide a framework for answering questions around how to design a certification system so that it is most likely to be effective. Next, we turn to these design choices.

IV. DESIGN CHOICES

Suggesting the idea of a certification body is only the beginning. Working from some operative theory of change and other substantive considerations, any certification approach then requires navigating a number of design choices. Here, we discuss five such choices, any of which can affect the nature and scope of certification.

A. PRESCRIPTIVE VS. DESCRIPTIVE

Certification regimes fall along a spectrum from descriptive to prescriptive. Descriptive systems seek only to provide objective, unbiased information, leaving it to the consumer to make the ultimate decision whether to purchase a product. Diamond certifications are descriptive—*any* diamond can be certified; the certification simply provides information about a diamond’s characteristics.¹⁰² Possessing that information, the purchaser is left to make whatever choice is preferred. As a result, for a descriptive certification to be meaningful, the consumer must have some sense of what the information means and how to use it. (Of course, even a descriptive certification is not value-neutral: there was a decision on the part of the certifier about what deserved to be evaluated and what information provided to the public.)

Prescriptive certifications are more evaluative, signaling that a product is satisfactory in a particular regard or that it conforms to a particular standard.

101. Marchant, *supra* note 61, at 136 (noting that successful certification schemes must give industry something of value to incentivize participation).

102. The leading diamond certifier is the Gemological Institute of America, which assesses diamonds on the basis of their color, clarity, cut, and carat (the “4Cs”), among other characteristics. See *Sample Natural Diamond Reports*, GEMOLOGICAL INST. OF AM., <https://www.gia.edu/analysis-grading-sample-report-diamond?reporttype=diamond-grading-report&reporttype=diamond-grading-report> (last visited Apr. 6, 2022).

B Corporations, discussed in Section III.B, are an example of prescriptive certification. A private organization called B Lab confers this certification on companies that have met standards relating to social and environmental performance, transparency, and other values.¹⁰³ Prescriptive systems tell consumers or potential purchasers that an independent third-party with relevant expertise has evaluated the product or company and has approved of it in a certain respect. Certified vendors essentially receive a gold star, and consumers don't have to do their own information gathering but can simply respond to the signal certification provides.

Depending on the operative theory of change and other considerations such as capacity, resources, and legitimacy, tech certification could be prescriptive, descriptive, or somewhere in-between. In the following example, we show what a prescriptive, descriptive, and hybrid regime (such as a system that rates or ranks products) might look like for certain aspects of automated license plate readers.

ALPRs are used to alert police when a *particular* wanted vehicle is detected.¹⁰⁴ But license plate reads also can be stored away, time-stamped and geo-located, to be fished out for investigative purposes.¹⁰⁵ Many people are concerned about the storage and use of this “historical data” to track individuals’ movements over time.¹⁰⁶ This concern could be mitigated partially by automatically deleting historical data after a set period of time, known as a “retention period.”¹⁰⁷ A shorter retention period means that an agency has less ability to track a vehicle’s movements over time.

The image on the following page indicates what a prescriptive, descriptive, and hybrid certification scheme might look like for ALPRs with regard to the retention period. (Of course, an entity certifying ALPRs would consider much more than just retention periods; we focus on them here for simplicity’s sake.)

103. See *About B Corp Certification*, B LAB, <https://bcorporation.net/about-b-corps> (last visited Apr. 6, 2022).






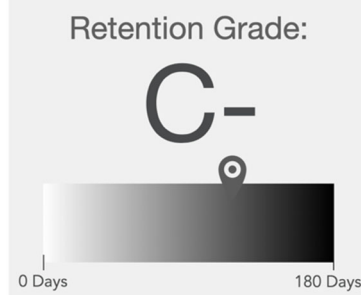
104. See *id.*

105. See *id.* at 5.

106. See *id.* at 24.

107. See *id.* at 34.

Table 2: Certification Approaches

ALPR 1: 28-day retention	ALPR 2: 120-day retention
<i>Prescriptive Certification: Retention period of thirty days or less is required for certification</i>	
 <p data-bbox="190 569 572 631">ALPR 1 has met the certification condition and is certified.</p>	 <p data-bbox="652 569 1076 631">ALPR 2 does not meet the condition and is not certified.</p>
<i>Descriptive Certification: Certifies all products</i>	
 <p data-bbox="215 904 549 966">Certification states ALPR 1's retention period of 28 days.</p>	 <p data-bbox="643 904 1088 966">Certification states ALPR 2's retention period of 120 days.</p>
<i>Hybrid Certification (Rating System): Certifier gives product a grade based on the length of retention</i>	
 <p data-bbox="171 1359 597 1421">ALPR 1 receives a higher grade for a shorter retention period</p>	 <p data-bbox="656 1359 1076 1421">ALPR 2 receives a lower grade for a longer retention period.</p>

One's theory of change will influence where along the prescriptive-descriptive spectrum a policing tech certification system should land. For example, if the theory of change is to influence vendors, then the certification system would need to be more prescriptive in design. As described above, prescriptive models (including hybrid models, such as rating systems) provide

a strong branding chip for certified vendors by signaling approval of their product. On the other hand, if the goal is to influence the public and regulators, then descriptive certification, which seeks to provide objective, unbiased information, may be better suited to bridging the information gap that these groups face.

Either approach—influencing vendors or influencing the public/regulators—could address the race to the bottom. Prescriptive (and hybrid) models directly incentivize vendors to improve their products so as to receive certification or obtain a high grade or rating. (However, this assumes that the certification criteria are transparent to vendors, which most, but not all, are.¹⁰⁸) Descriptive models indirectly incentivize vendors to improve their products, as public pressure forces policing agencies to choose to purchase (or not purchase) products based on the information that certification provides.

Ultimately, our research and discussions with stakeholders revealed strong skepticism around prescriptive-type certifications for policing tech because of these systems' norms-setting requirement. Many stakeholders expressed doubt that prescriptive systems premised on influencing vendors or policing agencies would produce a normative calculus that benefited communities. Others took issue with the very idea of establishing normative standards for issues like privacy or racial justice, arguing that there was no way to achieve consensus standards on such ethical dimensions. Stakeholders have different conceptions of what makes a product “ethical,” and the communities in which technologies are deployed may well disagree with a certification entity's conclusions and prefer to make their own determinations. Even if some imperfect baseline was established via a transparent process, consumers may misunderstand or put too much stock in what prescriptive certification represents—indeed, in the context of eco-certifications, there is a long-standing problem of “greenwashing”: the use of labels or certifications that misleadingly suggest that a product is environmentally friendly.¹⁰⁹

Finally, several stakeholders worried about the impact that prescriptive certification could have on criminal defendants seeking to challenge use of these technologies. Would an arrest that resulted from an agency's use of a certified product receive a thumb on the scale for its validity? As a result, many

108. Most certification regimes are transparent, but some (such as the Motion Picture Association of America's film rating system) apply *general standards*, as opposed to *precise rules*. This can undermine transparency by obfuscating the reasons for the entity's certification decisions. See Jeanne C. Fromer, *The Unregulated Certification Mark(et)*, 69 STAN. L. REV. 121, 142 (2017).

109. See HAMISH VAN DER VEN, BEYOND GREENWASH: EXPLAINING CREDIBILITY IN TRANSNATIONAL ECO-LABELING 64 (2019).

urged that any prescriptive certification would need to provide explicit disclaimers around the weight to give to its labeling in criminal adjudications.

Although stakeholders raised various concerns with prescriptive certification, significant consensus emerged around the need to inject the policing tech ecosystem with more reliable and objective information about these products. Law enforcement representatives described how the product information vacuum has forced them to rely on a sort of inter-agency rumor mill when seeking information about the utility of certain products. Civil liberties advocates, researchers, and government officials likewise bemoaned the absence of a trustworthy source for even basic information about these tools. Descriptive certification, with its emphasis on centralizing neutral information in a single entity, has the potential to fill these gaps. And because descriptive certification aims to disclose rather than evaluate information, it also largely can avoid the normative consensus traps that face prescriptive systems and hold space for different communities' needs and values by allowing jurisdictions to reach their own ultimate conclusions regarding ethical standards.

Still, descriptive systems are not without tradeoffs. They require policymakers (or the general public) to *interpret* the information disclosed. This places an evaluative burden on communities and policymakers, who, as discussed above, generally are not equipped with the expertise or tech literacy required to conduct a rigorous analysis. And without clear ratings and cross-product comparison, descriptive systems make it difficult for consumers to differentiate between products.

These concerns led some to prefer hybrid systems that both describe a particular product's qualities and provide some metric of comparison to a standard. For example, one stakeholder suggested borrowing from food nutrition labeling in which a single label both describes the nutrition content of the particular product and compares it to the recommended daily nutrient allowance. There even was a suggestion that the concerns raised by trying to certify "ethical" policing tech could be avoided by turning the entire project on its head to certify only the worst offenders, giving out stamps of *disapproval* for products that clearly are beyond the pale.

B. EVALUATING EFFICACY

How would a tech certification entity evaluate products' efficacy? This depends on a number of factors—what the theory of change is, whether the certification is descriptive or prescriptive, the availability of data upon which to base conclusions about efficacy, and the entity's resources and expertise, to name a few. Perhaps the most important factor—and the thorniest to

resolve—is how one defines “efficacy.” And defining this term carefully is essential because a certification entity’s definition can affect how vendors design their products and how those products are perceived by policymakers and the public.

First, a certification entity simply could evaluate a product’s specifications—i.e., does it do what it says “on the tin.” For example, how long can a drone remain airborne without requiring recharging? How accurately does an ALPR read a license plate? Law enforcement representatives we spoke to repeatedly observed that this information would prove quite useful in their procurement and deployment decisions. They were hardly alone; advocates likewise expressed frustration with the lack of available objective information on whether these products fulfill their basic technical promises. Many welcomed the prospect of a certification system that might step into this void and help encourage minimum viable technical standards for these policing technologies.

There are serious challenges posed by even this minimal version of efficacy review: (1) it is extremely expensive to develop test suites to evaluate these products; (2) efficacy testing always is contestable; (3) it requires some sort of apples to apples comparison across a product line, and it’s unclear if that is even as feasible with policing tech as it is with, say, vacuum cleaners; and (4) AI and ML technologies raise a host of domain transfer issues—for example, which dataset would serve as the measurement baseline (training? testing? deployment?) with pros and cons to each. Add to that the difficulties posed by the need to frequently re-evaluate in the face near-constant software and hardware updates. Some machine learning tools even continuously learn in the field—in essence, as the model ingests deployment data, its pattern regulation algorithm changes. Even without the bureaucratic obstacles facing hard law, it would be challenging to design a certification system that is flexible enough and has the capacity to assess such continuous product change.

Some stakeholders suggested some of these issues could be addressed by placing the burden back on the vendor, for example, by requiring self-evaluations and self-attestations of conformity to a standard rather than requiring the certifier to conduct the testing itself.

Even assuming the practical problems with an approach that measures basic technical efficacy could be resolved, there still are limits to its utility as the sole measure of efficacy. For example, the accuracy of ALPR reads is surely an important consideration, but it says relatively little about whether deploying ALPRs would be *useful* in achieving public safety. Many experts felt strongly that efficacy is a useless metric unless it communicates something about the actual operational value of the tool.

Second, a certification entity might evaluate a product's impact on crime-fighting by attempting to tie product use to policing metrics such as cases cleared or crime deterred. This, too, may prove to be vital information, especially if this efficacy evaluation enabled comparisons across product lines to determine which type of tool actually is more likely to have a positive impact on crime-fighting. For example, both face recognition and fingerprint identification are biometric tools used to identify suspects. Imagine a certification system that was able to aggregate and report out data on successful suspect identifications by face recognition and fingerprint with breakdowns by agency or jurisdiction, perhaps as compared to system cost. This kind of comparative information could guide agencies in choosing which tools to procure or inform legislative decisions around law enforcement budget allocations. It also could inform and empower advocacy campaigns by providing some factual basis for what affects crime-fighting and what doesn't.

But to conduct such an analysis, the certification entity must have *access to data*. Many agencies don't generate such data in the first place, let alone turn it over to independent researchers. And even if the data is generated, answering these questions as an empirical matter can prove very difficult. If (and it is a big "if") one measures crime fighting by the number of crimes reported to police, how is causation established? That is, how can one be sure that changes in the crime rate are attributable to the vendor's product? There are methods of determining causality in the social sciences, but the challenges to doing this are not insignificant.

Third, and most ambitiously, tech certification could evaluate a product's overall effect on public safety. This raises a litany of thorny questions. How does one define and then measure public safety? The number of cases closed? The amount of crime deterred? Community surveys? What about the *positive* civil rights impact of technology, such as the use of technology to constrain officer discretion or enable better oversight?

Using ALPRs again as the model, the graphic below visualizes these three approaches:

Table 3: Approaches to Evaluating Efficacy

<p>Evaluate product specifications: For example, evaluate the accuracy of ALPR plate reads or the algorithmic bias of face recognition</p> <p>Daytime Accuracy: Pass (95%)</p> <p>Nighttime Accuracy: Pass (90%)</p>																	
<p>Evaluate impact on policing metrics: For example, evaluate clearance or arrest rates</p> <table border="1"> <thead> <tr> <th colspan="3">Clearance Rates</th> </tr> <tr> <th colspan="3">Based on data from 20 agencies, Jan. 2023–Dec. 2023</th> </tr> <tr> <th></th> <th>Property & Vehicle Offenses</th> <th>Violent Offenses</th> </tr> </thead> <tbody> <tr> <th>With ALPR</th> <td>30%</td> <td>50%</td> </tr> <tr> <th>Without ALPR</th> <td>24%</td> <td>52%</td> </tr> </tbody> </table>			Clearance Rates			Based on data from 20 agencies, Jan. 2023–Dec. 2023				Property & Vehicle Offenses	Violent Offenses	With ALPR	30%	50%	Without ALPR	24%	52%
Clearance Rates																	
Based on data from 20 agencies, Jan. 2023–Dec. 2023																	
	Property & Vehicle Offenses	Violent Offenses															
With ALPR	30%	50%															
Without ALPR	24%	52%															
<p>Evaluate overall impact: Measure the overall impact on public safety, however conceived</p> <p>Public Safety Impact: High</p>																	

There is one final possibility that shifts the burden of proof to vendors and could lead to far more available information: certification could set rules about *how* vendors make claims about product efficacy. For example, a certification entity could require that vendors only make efficacy claims that have been vetted by independent researchers. Or it could require that vendors publicly disclose all data upon which efficacy claims are based, opening such claims up to public scrutiny. In this vein, certification could enforce a sort of “truth in

advertising” requirement, similar to requirements enforced by the Federal Trade Commission. Alternately, certification even could tell vendors what they *must* advertise on the tin, including the nature of oral representations they can make in marketing their products—akin to the requirements that prescription drug labels and advertisements list certain warnings and precautions.¹¹⁰

C. “USE” CASES

One of the great challenges of certifying policing technologies is whether to certify only the product in the abstract or to take account of particular uses of the product. Some certification schemes are contextual, others are not. Cheese, for example, might be certified as Kosher, but that does not preclude putting it on a bacon cheeseburger. On the other hand, Leadership in Energy and Environmental Design (LEED), a green building certification program, only certifies entire buildings as eco-friendly; it does not matter if all “green” materials were used, it is the way in which these materials come together into a building that counts.¹¹¹

When it comes to policing tech, context is of great importance. The ethical implications of a policing technology turn largely on two contextual use factors. First there is the issue of how individual agencies choose to use the particular product. The very same ALPR can be used by one agency only to detect vehicles wanted in connection with serious felonies but by another to generate fines and fees revenue, which fall most heavily upon predominantly minority neighborhoods. Second, there is the issue of how a technology is used in conjunction with *other* technologies—that is, how a technology integrates into a larger *system*. For example, ALPRs have been used in conjunction with aerial surveillance to enable more precise tracking of vehicles’ movements.

In short, certifying uses is difficult. They are very dependent on both the individual and systemic contexts of a given jurisdiction. To truly prove valuable, some have argued that a certification agency would have to certify products for different uses, in different combinations, in different jurisdictions. Both the decision to certify use cases, and its implementation, pose difficult challenges. Here are a few potential routes a certification entity might take in addressing use cases.

110. See Michael J. Lopez & Prasanna Tadi, *Drug Labeling*, NAT’L CTR. FOR BIOTECHNOLOGY INFO., <https://www.ncbi.nlm.nih.gov/books/NBK557743> (Aug. 19, 2021); *Drug Advertising: A Glossary of Terms*, U.S. FOOD & DRUG ADMIN., <https://www.fda.gov/drugs/prescription-drug-advertising/drug-advertising-glossary-terms> (last visited Apr. 6, 2022).

111. See *Green Building 101: What is LEED?*, U.S. GREEN BLDG. COUNCIL, <https://www.usgbc.org/articles/green-building-101-what-lead> (Dec. 16, 2020).

1. *Don't address use cases*

The first option is simply to ignore use cases. For example, certification of ALPRs could assess devices on the basis of plate read accuracy and data security, while sidestepping the questions of how, for what purpose, and in what combinations agencies use ALPRs.

The value of even such a limited approach should not be discounted. It would be valuable to have a credible, independent entity evaluate how accurately an ALPR reads a license plate, how well a predictive policing algorithm performs, or how biased (or unbiased) a facial recognition system is. Indeed, this is why the NIST tests and ranks the accuracy of face recognition algorithms. It would make little sense for each individual jurisdiction to make such assessments on its own.

There are additional benefits to this approach. A certification scheme that ignored use cases would be far easier to design and implement. And, for better or for worse, it would leave it to local policymakers to decide which use cases and combinations were permissible.

Still, when it comes to policing tech, how it is used is often every bit as important as whether it works when it is used. An algorithm that is free of racial bias could be used by agencies in a way that gravely exacerbates racial disparities (for example, for the purpose of enforcing low-level drug offenses). At present, there is little transparency around, let alone local regulation of, how agencies use policing technologies. In many (and perhaps most) jurisdictions, if the certification entity were not addressing use cases, no one would be. Many experts we spoke with questioned whether a certification system would provide any meaningful value if it did not address use cases.

2. *Certify products, addressing use cases indirectly through product design*

Second, without certifying use cases directly, certification could influence product design, which in turn can affect use cases.

For example, certification could be conditioned on the implementation of features that encourage or require agencies to be transparent about uses—both individual product uses and use in combination with other tools. If, for example, the concern is that agencies will use drones to surveil protests and other expressive activity, vendors could be required, as a condition of certification, to create transparency portals—that is, online portals disclosing information about police use of technology—through which agencies could (or must) disclose the time and flight path of each drone flight. In this way, the public would have the tools to draw conclusions about uses on their own. Also, the fact that the information would become publicly available might cause policing agencies to be more careful about their uses.

But there are limits to this approach as well. Transparency is, of course, vitally important to the effective regulation of policing agencies. Yet for transparency to lead to sensible use limitations, action still is required—by policymakers and regulators enacting reforms, by communities and civil society groups making demands of agencies, by aggrieved citizens challenging agencies' actions in court, and so on. Transparency may well lead to such efforts, but this cannot be taken as a given.

Alternatively, certification of a product might require vendors to implement design safeguards that restrict the ability of agencies to engage in certain problematic uses. For example, one way to curtail agencies' ability to conduct location tracking using ALPR historical data would be to design the device such that data was automatically deleted after seven days. Such features are, in a sense, self-auditing.

Even with this approach, though, some uses may be difficult to address through product design. Suppose that a certification entity wanted to limit the use of historical ALPR data, allowing its use only in the investigation of serious offenses. How is a vendor to design its product to allow use of historical data for serious offenses but disable agencies from running historical searches to investigate minor vandalism or graffiti? One answer is that the software could simply ask the user what the purpose of the historical search was and record that information. This, combined with a transparency mechanism, might do the trick—although there are of course always some lingering questions about the candor of all users and agencies.

3. *Directly certify use cases*

Third, the certification entity could certify use cases directly—that is, conclude that a product is certified for a specific intended purpose, when used in a specific intended way. For example, an ALPR could be certified for use in connection with the enforcement of felony offenses through the use of hotlist alerts but not certified for use in low-level enforcement. Certification also might limit the use of a product in conjunction with other technologies.

In such a scheme, the certification entity could play one of two roles. It might simply state the use cases and combinations for which a product is certified, leaving it to communities and policymakers to ensure the local agency user complies with the restrictions.

Alternatively, a certifier could enforce compliance with certified use cases. The entity might require vendors to regulate agency use through terms of service, for example. Or the entity could certify products agency by agency—i.e., certify an ALPR for use by the Whoville Police Agency because it has adopted appropriate use policies and training protocols, but not for the

Whereville Police because they have not. However, this approach would entail significant expense and, absent a vigorous program of compliance review, may not be successful anyway.

An entirely different approach to the problem of use would be to issue non-certification for certain use cases where the costs outweigh the benefits or cannot be adequately mitigated through design safeguards or other restrictions. And like an FDA drug label, tech certification labels could come with warnings about the potential risks of any non-certified uses. This approach also could be applied to target the issue of systemic use risks—the label could provide warnings about the risks of combining certain technologies, just like drug labels may warn about combining drug use with alcohol. And still another option might be certifying whether the user is qualified to use a given technology.

Table 4: Options for Addressing Use Cases

Don't address use cases		<ul style="list-style-type: none"> • Pros: Ease of design and implementation • Cons: More limited value
Address use cases through design	Design features that create transparency/accountability around agency uses	<ul style="list-style-type: none"> • Pros: Information-forcing • Cons: These features may not lead to substantive change
	Design features that restrict agency uses	<ul style="list-style-type: none"> • Pros: Limits use cases without auditing • Cons: Impractical for certain use cases
Certify use cases	Certify products for specific use cases	<ul style="list-style-type: none"> • Pros: Gives guidance to communities • Cons: Lack of enforcement mechanism
	Certify products for specific use cases + enforcement	<ul style="list-style-type: none"> • Pros: Effective at addressing many use cases • Cons: High cost

D. SUBSTANTIVE DESIGN STANDARDS

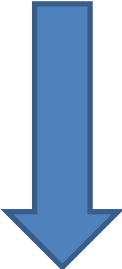
Both descriptive and prescriptive certifications apply substantive standards. In prescriptive certification, a product passes or fails based on those standards. But even descriptive systems incorporate substantive standards. Gem certification, for example, relies on substantive standards to determine whether a gem should be classified as pink or red. Likewise, a policing tech

certifier would need to decide which traits of a technology to evaluate, such as data retention, accuracy, and the like.

Substantive standards are yet another design choice, and careful thought must be given to how those requirements are designed. Should certification be directed towards giving agencies and jurisdictions choices, or should those choices be made by the certification entity?

Suppose, for example, that a certification entity determined that ALPRs should be evaluated on whether they include a transparency portal through which agencies disclose information about their ALPR use to the public. The question then arises whether certification should make the portal's use mandatory for agencies, or whether the tool should just be part of the device, but its use by any given agency wholly voluntary. Then, even in the latter case, there is the question of whether the certification agency should include “nudges” to encourage agencies to use the portal. Nudges use design architecture to encourage users to make better decisions. How options are presented to users and which ones are enabled or disabled by default may have a profound influence on the decisions an agency ultimately makes.

Table 5: Examples of ALPR Safeguards

Choice: The vendor includes a transparency portal for agencies to use <i>if they so choose</i> .	 <p style="margin-left: 100px;"><i>Stronger Requirement</i></p>
Choice + Nudge: The transparency portal <i>is enabled by default but can be disabled</i> by the agency.	
No Choice: The transparency portal is included and there is <i>no way to disable it</i> .	

At first glance, the “No Choice” safeguard might seem best. Agencies are left with no choice but to include the safeguard or meet whatever substantive standard the certification agency puts in place.

The reality is more complex, in large part because substantive design choices interact with stakeholder buy-in for the certification system—an issue we discuss further in Sections IV.A–B. For example, suppose that a certification entity required vendors to use the “No Choice” safeguard. Each vendor then will decide whether to get certified and comply with this strong restriction. The basis for the vendor's decision will depend in great part on whether the certifier has market power. If the certification standard has been adopted widely by agencies and industry, the vendor may have little choice but

to acquiesce in the “No Choice” safeguard. If, however, the certification entity is an upstart, or the vendor faces brisk competition from another vendor that does not get its products certified, the vendor may well decide to forego certification. If enough vendors forego certification, the impact of the certification scheme may be diminished.

One further point to consider is that a certifier’s substantive requirements can limit the options available to regulators and communities—products become “one size fits all.” This is hardly unique—consider, for example, the existence of federal laws that set uniform minimum standards across the United States (e.g., federal labor law and the federal minimum wage). Yet there are costs to this approach. If communities feel that certification fails to strike the right balance, they won’t be amenable to following the guidance of certification. Alternatives might be to have local or statewide bar-setting or to outsource substantive standard development to trusted expert groups.

E. INSTITUTIONAL DESIGN OF CERTIFICATION ENTITIES

Certification regimes differ markedly in the extent to which they are independent from industry and include community stakeholders. In some regimes, industry dominates the standards-setting and certification process, while other entities seek to ensure balanced power-sharing. These contrasting approaches are exemplified by the two certification regimes discussed below: the International Sustainability and Carbon Certification and Fairtrade.

Table 6: Governing Certification: Two Contrasting Approaches

	
<p>The International Sustainability and Carbon Certification is governed by a 150-member association. 90% of its members are producers, processors, or others involved in the supply chain. The organization's Board consists only of industry representatives and two researchers.¹¹²</p>	<p>Fairtrade is governed by the organization's General Assembly and Board. Producers and national Fairtrade organizations (which raise awareness and administer the standard) have equal representation in the organization's General Assembly and Board, leading to balanced power-sharing.¹¹³</p>

If the theory of change envisions vendor engagement with certification as the lever, then industry requires a significant place at the table. Vendors scarcely can be expected to participate in a certification scheme that doesn't adequately represent their interests.

Whereas if the theory of change envisions legislators or the public as the target audiences, then there may be less of a need to have vendors fully on board. To be sure, some certification entities evaluate products without the vendors' cooperation—for example, an entity focused on evaluating household products might purchase a product independently, before rating it or giving it a seal of approval. That, in a sense, is how Consumer Reports operates.¹¹⁴

This approach would face unique difficulties in the current policing technologies marketplace. Most policing technologies cannot be bought from a store shelf. Some agencies we spoke with, particularly federal law enforcement, cited national security concerns with disclosing policing tech information. The vendor also often has (or least, claims) proprietary reasons to keep product information under wraps, backed by trade secret/IP law. Consequently, evaluating such products may require the vendor to submit

112. GREENPEACE, *DESTRUCTION: CERTIFIED* 54 (2021).

113. *Our General Assembly and Board*, FAIRTRADE INT'L, <https://www.fairtrade.net/about/ga-and-board> (last visited Apr. 6, 2022).

114. *See Research and Testing*, CONSUMER REPS., <https://www.consumerreports.org/cro/about-us/what-we-do/research-and-testing/index.htm> (last visited Apr. 6, 2022).

willingly to the certification process. Otherwise, the entity would be forced to conduct product evaluations on a slim public record. Even so, it is hard to imagine the development of a system that cuts vendors out entirely.

Nonetheless, there are obvious dangers if certifiers becoming too cozy with industry. Overrepresentation of industry in certification schemes can lead to capture, resulting in ineffectual standards and lax auditing.¹¹⁵ Moreover, capture by industry comes at the expense of other stakeholders—such as representatives of the communities that are most affected by policing. Balanced representation within the certification entity and its governing body would be crucial in ensuring that all stakeholders' interests are accounted for adequately.¹¹⁶

There are many ways in which a certification entity could implement mechanisms for public participation. For example, an entity might implement a notice and comment period during which interested members of the public could give feedback regarding proposed standards. Another possibility is the creation of a grievance process, by which the public could file complaints in relation to harmful uses of policing technologies—this information could guide future standards-setting and certification decisions. Such mechanisms might afford affected communities meaningful opportunities to participate in the standard-setting and certification processes and ensure that industry players with deep pockets and the time to dedicate to lobbying do not end up dominating the process.

F. PUBLIC OR PRIVATE

Finally, there is a choice to be made regarding whether certification ought to be administered by a *private* or *public* entity. Most certification regimes are administered privately. That is true of B Corporations, LEED, Fairtrade, and many others. Still, there are some notable exceptions, such as Energy Star, the energy efficiency standard administered by the U.S. Department of Energy.

In our research, we encountered significant skepticism around private entities administering a policing tech certification. This skepticism emerged from civil rights advocates, community activists, and tech vendors alike. Chief among these concerns was how the entity would be funded; if the answer was industry, many warned that issues of conflicts of interest and capture would be unavoidable and unmediatable. Others noted that institutional trust in policing agencies and Big Tech is low, especially from communities most impacted by policing tech, such as Black communities. Thus, for the entity to

115. See GREENPEACE, *supra* note 112, at 11.

116. See K. Sabeel Rahman & Jocelyn Simonson, *The Institutional Design of Community Control*, 108 CALIF. L. REV. 679 (2020).

have legitimacy in the eyes of the public, it cannot be seen as being in bed with either policing agencies or tech vendors. And the need for this entity to have teeth or enforcement power also counseled in favor of a public program with its penumbra of hard law in the background.

Consensus emerged that the certifier role should be played by a public entity. There is much to be said for public certification. It may engender more trust from the public and more naturally addresses concerns about the democratic legitimacy of certification.¹¹⁷ Moreover, public certification could have a profound and immediate effect on the market, especially if certification were tied to federal funding for policing agencies. Of course, this leaves certification vulnerable to the vicissitudes of politics. In early 2017, for example, the Trump administration sought to end the Energy Star program; in early 2021, the Biden administration sought to expand it.¹¹⁸

The question is whether a public approach is viable. It would take political energy to get it adopted, and the currently anemic regulatory environment suggests legislators don't have the stomach for stepping into this space. On the other hand, the existing regulatory lacuna likely is not the product of legislative disinterest, but self-interest. As discussed above, the topic of policing is both polarizing and highly salient to voters; comprehensive reform through legislation is a risk that many legislators may not be willing to take.¹¹⁹ It is precisely for this reason that legislators may prefer to offload the issue to some sort of regulatory agency or certification body. As Lisa Schultz Bressman has observed:

Congress might attempt to avoid blame for controversial policy choices by shifting them to agencies, while still claiming credit for broad solutions to public problems. In other words, Congress might aim to write just enough policy to receive a positive response for its

117. See Marchant et al., *supra* note 61, at 130; see also Hagemann et al., *supra* note 59 (discussing public-private models of certification).

118. See Nives Dolšak & Aseem Prakash, *The Trump Administration Wants to Kill the Popular Energy Star Program Because it Combats Climate Change*, WASH. POST (Mar. 23, 2017), <https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/23/the-trump-administration-wants-to-kill-the-popular-energy-star-program-because-it-combats-climate-change>; Tik Root, *Biden Administration Announces New Energy Star Standards, Plans for Emissions Targets for Federal Buildings*, WASH. POST (May 17, 2021) <https://www.washingtonpost.com/climate-solutions/2021/05/17/biden-energy-efficiency>.

119. See generally Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; or, Why Don't Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079, 1089 (1993).

actions, while deflecting any negative attention for the burdensome details to the agency.¹²⁰

Whether public or private, the entity would face a key capacity challenge: the type of evaluation envisioned requires diverse expertise and technical experience that currently is in short supply across the public and private sectors. Putting aside all the challenges around standing up such an entity, the question remains: who would staff such an entity?

V. CHALLENGES

Thus far, we have been considering what design choices would have to be made to get a certification body going from the ground up. But once the choice is made to proceed with a certification entity, there still will be challenges. This Part discusses some key challenges faced in setting up a certification body and suggests what could be done about them.

A. GAINING LEGITIMACY AND CREDIBILITY: PUBLIC BUY-IN

Certification systems naturally raise concerns about democratic legitimacy. Most standard-setters and certifiers either are several steps removed from direct democratic processes (if certification is run by a public agency) or are entirely separate from them (if run by a private entity).¹²¹ Consequently, whether the system is publicly or privately run, the public may feel shut out of the certification process and/or that industry has too much sway.¹²² This matters: if certification is to wield any influence over how policing technologies are designed and regulated, communities and policymakers must trust the certifier.

There are elements of certification design that can help ensure meaningful public voice and representation. As an initial step, basic transparency around

120. Lisa Schultz Bressman, *Chevron's Mistake*, 58 DUKE L.J. 549, 568 (2009).

121. See Lytton, *supra* note 67, at 569; Kenneth W. Abbott, *Introduction: The Challenges of Oversight for Emerging Technologies*, in INNOVATIVE MODELS FOR EMERGING TECHNOLOGIES (2014); Doris Fuchs, Agni Kalfagianni, & Tetty Havinga, *Actors in Private Food Governance: The Legitimacy of Retail Standards and Multistakeholder Initiatives with Civil Society Participation*, 28 AGRIC. HUM. VALUES 353 (2011) (noting that regulatory agency rule enforcement is subject to attenuated “legitimacy chains” as regulatory power is delegated to bureaucrats); Gutierrez, *supra* note 98, at 144–45 (observing that the fact that “any organization” can create a soft law system can raise legitimacy issues) ¶; Hagemann et al., *supra* note 59, at 98–99 (discussing legitimacy issues that even may face public approaches to soft law governance).

122. See Marchant et al., *supra* note 37, at 9.

the certification process can foster public legitimacy and credibility.¹²³ This ideally occurs at every step of the process—from initial standard-setting to individual certification decisions. Transparency, in turn, can breed accountability. For example, some have argued that certification entities should publish the reasoning behind their certification decisions, creating a body of binding precedent that enhances procedural fairness.¹²⁴

Certification systems can, and should, go a step further by actually soliciting and incorporating public input on their certification standards and process. For example, the Sustainable Forestry Initiative, which certifies sustainable forestry practices in the United States and Canada, subjects its certification standards to review every five years in a process that includes an opportunity for public review and recommendations.¹²⁵ Another major player in the certification world, Underwriters Laboratories, opens its standards creation and revision process to any interested party and actively empanels a broad set of stakeholders across industry, technical experts, and consumers to review all suggestions.¹²⁶ Its panels also request and respond to public comments, and it publicly releases its standard-setting activities.¹²⁷ When designed with such open participation guarantees, voluntary certification may in fact be “more directly democratic than the state regulatory apparatus.”¹²⁸ Participatory mechanisms also can address the problems of capture and representational imbalances, as discussed in Section III.E. But just as important, they are a means to hold the certifier itself accountable and enhance its standing among the relevant stakeholders.

In short, public legitimacy presents a difficult but not insurmountable challenge for certification systems whether they are administered by private entities or public agencies.

B. ACHIEVING UPTAKE: AGENCY AND VENDOR BUY-IN

Successful certification systems typically provide value to both the producers and consumers in the target marketplace. The ethical policing tech

123. *Cf. id.* at 12 (explaining that a mechanism for making soft law more effective and credible may include “transparency in demonstrating compliance”).

124. Fromer, *supra* note 108, at 190.

125. Cary Coglianese, *Environmental Soft Law as a Governance Strategy*, 61 JURIMETRICS J. 37–38 (2020).

126. Lytton, *supra* note 67, at 569.

127. *Id.*

128. Tracey M. Roberts, *The Rise of Rule Four Institutions: Voluntary Standards, Certification and Labeling Systems*, 40 ECOLOGY L.Q. 107, 140 (2013); *see also* Gregory N. Mandel, *Regulating Emerging Technologies*, 1 L. INNOVATION & TECH. 75, 90 (2009) (“Broad stakeholder outreach and dialogue can bring credibility, new ideas, current information, continual feedback, and public trust to a governance system.”).

marketplace presents an interesting wrinkle in that the consumers are bifurcated: agencies, who are (typically) the buyers, and the public, who is the end-user (or end-used-upon). At present, the public largely is cut out of the producer-consumer relationship. Vendors deal directly with agencies, and this feedback loop mostly ignores ethical harms. The purpose of certification is to inject ethical concerns into this loop by explicitly evaluating them and thereby making them marketable. Success then depends on the degree to which key stakeholder groups—tech vendors, agencies, the public—value the information certification provides. As discussed above, value to the public will hinge on legitimacy and credibility issues.

For agencies and vendors, the value calculus raises different, albeit related, questions. Will agencies find enough value in certification’s potential to reduce public backlash to choose certified products even when legislation or their own policies do not require it? Some law enforcement representatives we spoke with indicated this incentive may not be powerful enough to cause agencies to alter the status quo. Similarly, will a critical mass of vendors deem there to be sufficient brand value from ethical labeling to undergo certification? Or will the lack of a requirement on the agency side to purchase certified products defeat buy-in? These buy-in issues may dictate, or at least greatly impact, the design of the certification system. For example, a certification entity might choose to design a prescriptive certification system rather than a descriptive one to ensure vendor buy-in to the system.

Or take setting certification criteria for ALPR data retention. Standards that are too rigorous might impede initial adoption of the standard by vendors concerned by limiting their customers’ choices. Interestingly, if a certifier does have market power, vendors may have an incentive to encourage it to raise certification standards in order to entrench their own market power.¹²⁹ For example, an ALPR vendor might favor a standard requiring advanced analytics of racial and socioeconomic disparities resulting from ALPR use, a feature that upstart competitors may lack the resources to implement in their own products. However, raising the bar in this way only goes so far; monopolization of a product category by a vendor may stagnate innovation not only in the product’s core features but in its safeguards and accountability features as well.¹³⁰

129. For example, small watchmakers in Switzerland complain that the standard to certify a watch as Swiss-made is too rigorous and intentionally designed to shield the country’s dominant watchmakers from competition. See Fromer, *supra* note 108, at 150–51.

130. See generally Elizabeth Joh & Thomas Joo, *The Harms of Police Surveillance Technology Monopolies*, DENVER L. REV. F. (forthcoming 2022) (“When a particular technology has only a

When it comes to certification uptake by vendors and agencies, there is also something of a critical mass conundrum: buy-in by stakeholders begets buy-in, but getting over that initial hump to create a system with sufficient market power to encourage additional participation may be a Sisyphean task.

C. COMPLIANCE AND ENFORCEMENT

Certifiers face a dilemma: how does a certification entity ensure that vendors comply with certification requirements, especially over time? This is no small matter because failure to enforce certification requirements can diminish the certifier's credibility and undermine the reason for having certification in the first place.¹³¹

Enforcing certification requirements is easier said than done. Because certification typically is voluntary, certifiers must rely mostly on carrots, not sticks, to ensure compliance.¹³² (Weak enforcement may be especially acute for private certifiers; if the system were run by a federal agency, as proposed by FAS and discussed above, industry may be warier of failing to comply with a program that has the imprimatur of a government agency.)

Regardless of whether the certification entity is public or private, certification systems have developed methods of monitoring compliance that could be applied in the policing technology context. These include:

- *Tip Programs*: The certifier could set up a program to solicit tips from the public regarding violations of certification requirements. For example, if an agency's drone fleet is certified for use only in connection with active crime scenes, citizens could report that the agency was using the drones to monitor political protests.
- *Audits*: Regular audits of tech vendors and/or the agencies using their products could be a requirement of certification. (This might be part of the certifier's contract with vendors—vendors must submit to audits as a condition of using the certification mark.) For example, a certifier could require that ALPR users provide a reason for performing any historical searches. The certifier then could require the vendor to provide a representative sample of these audit trails at

sole provider, it may be of low quality: the technology may still be maturing, or the lack of competition has reduced incentives to improve it.”)

131. As Gary Marchant explains, though, enforcing certification requirements is easier said than done: “design and implementation of a cost-effective post-market surveillance system is difficult, due in large part to the ‘noise’ inherent in studying complex and diverse real-world situations.” Marchant et al., *supra* note 61, at 150.

132. *See id.* at 136; *see also* Roberts, *supra* note 128, at 146 (observing that voluntary certification systems can “encourage” compliance with their requirements but lack mandatory enforcement powers).

regular intervals to determine if the vendor's clients were running searches for impermissible purposes.

- *Sanctions:* Companies that violate certification requirements can have their certification revoked. Stakeholders we spoke to urged the use of contracting leverage to implement enforcement: agencies or vendors could incorporate clawback clauses that make ethical requirements or certification compliance part of the performance clause. And some certifiers even have sued vendors for violating requirements while using the certification mark on a theory of trademark dilution.¹³³ The gravest sanction may come from the court of public opinion—certifiers could publicize gross violations through media and public relations campaigns.

Choosing adequate enforcement and compliance mechanisms are important, but they are only part of the battle when it comes to ensuring a policing tech certification is doing its job. The other half of the battle is an issue that also stymies hard law regulation: figuring out ways for certification to keep pace with these rapidly changing technologies. Still, with the right design thinking and vendor cooperation, there likely are ways to implement regular monitoring. And even if the certification merely set a regular re-certification schedule (annually or every two years) rather than some kind of close-to-live monitoring, this would represent a significant improvement over the status quo in which there are no rules or requirements around product auditing.

D. FENDING OFF REGULATION

As discussed above, certification both can *complement hard law systems* (or fill gaps in them) and *facilitate the adoption of hard law*. The problem is that creating a certification body also may have the exact opposite effect: warding off the adoption of hard law.¹³⁴ By signaling to regulators and the public that the problems presented by these products are being addressed, certification systems can disincentivize further regulatory action. For example, in response to public backlash about violent video game content, tech companies created

133. See Trevor T. Moores & Gurpreet Dhillon, *Do Privacy Seals in E-Commerce Really Work?*, ACM (Sept. 28, 2021), <https://cacm.acm.org/magazines/2003/12/6646-do-privacy-seals-in-e-commerce-really-work/fulltext>.

134. See Carlos Ignacio Gutierrez & Gary Marchant, *Soft Law 2.0: Incorporating Incentives and Implementation Mechanisms Into the Governance of Artificial Intelligence*, OECD.AI: POLY OBSERVATORY (July 14, 2021), <https://oecd.ai/en/wonk/soft-law-2-0> (discussing reasons why organizations comply with soft law programs and observing that “[o]ne incentive is to avoid inflexible hard law requirements that would otherwise kick-in”).

a rating system that successfully placated federal and state lawmakers “who were pitching a variety of more formal restrictions on youth access to video games.”¹³⁵ Today, this industry-developed ratings system remains the “primary governance mechanism in this arena.”¹³⁶ In fact, scholars have noted that certification’s potential to stave off hard law often serves as a key incentive for organizations to submit to these systems.¹³⁷

There are two things that can be said here. The first is that a successful certification system may eliminate the need for hard law. That arguably was the case with the video game example. (Studies show that children “spend less time playing violent video games when their parents use the rating system to guide purchases and set rules for video game play.”)¹³⁸ And indeed, certification may be better in some instances than regulation. Unlike the traditional regulatory process, certification has the ability to bring together a broad coalition of stakeholders and subject matter experts in a non-adversarial process to devise the rules of the road. Lest we forget, legislative efforts are subject to watering down from industry interest groups and partisan divisions alike. Through its multistakeholder and more flexible process, certification presents an opportunity to set a higher or more precise bar for the industry standard.

However, not all the problems with policing tech can be solved by certification alone. For certification to be viable, it must not undercut government regulation of the police. Rather, certification should be designed in a way that *stimulates* and serves as a model for the development of hard law.

First, the certifier could focus on areas in which a lack of information has most impeded effective regulation. For example, very little is known about how useful ALPR historical data is to policing agencies. A certifier could require vendors to produce aggregated statistics about historical data use—how often agencies use data older than thirty days, for example—which could provide valuable insights to lawmakers.

Second, the certifier could itself engage in advocacy. Consumer Reports, for example, has an advocacy arm that lobbies for consumer protections on a number of fronts. A policing tech certifier might lobby for more hard law

135. Adam Thierer, *Soft Law in U.S. ICT Sectors: Four Case Studies*, 61 JURIMETRICS J. 79 (2020).

136. *Id.*

137. See Gutierrez et al., *supra* note 121, at 137 (“Firms can endeavor to sidestep hard law by developing soft law that eases society’s reservations about their products or services.”).

138. IOWA STATE UNIV., *Video Games Ratings Work, if You Use Them*, SCI. DAILY (Jan. 25, 2017), <https://www.sciencedaily.com/releases/2017/01/170125145805.htm>.

regulation of policing tech and could draft model legislation requiring agencies to use the safeguards that the certifier requires vendors to implement.

Although a policing tech certification entity should be mindful of warding off regulation, making effort to incorporate design choices that would support or complement hard law, it is not a reason to derail further exploration. As several stakeholders pointed out, even without any soft law measures on the horizon, policymakers thus far have abdicated their responsibility for regulating policing technologies.

E. NORMALIZING TECHNOLOGIES

There also is a concern that any governance system that engages with these technologies in any way—even if it is to try to mitigate the ethical harms they present—risks validating or further entrenching their use. For this reason, some believe that the only way to mitigate the harms of law enforcement use of these tools is to ban them outright.

But this argument rests on a few questionable premises: (1) that these tools are not already being normalized, (2) that there are not sufficient public safety benefits to extract from these tools assuming the necessary safeguards are in place, and (3) that there is sufficient political and public will to enact widespread bans.

Despite significant advocacy campaigns to ban FRT, one of the most high-profile surveillance tools, fewer than two dozen jurisdictions across the country have passed bans.¹³⁹ And this movement is up against majority opinion—a Pew Research Center poll found that 56% of Americans trust law enforcement will use this tool responsibly. In the meantime, law enforcement use continues unchecked.

Still, FRT is only one technology, albeit an understandably controversial one; believing that all policing technology would be banned is a form of magical thinking. The status quo is a world in which police are using these technologies while regulators are sitting on their hands. Certification at least presents a potential path forward to a world in which regulators have the information and motivation required to act and agencies are incentivized to acquire tools that are designed with safeguards in place to protect civil rights and liberties concerns. And a certification system need not certify every technology. It may very well decide that there are some tools that simply are too harmful or risky to merit evaluation. In doing so, certification could create

139. *Map*, BAN FACIAL RECOGNITION, <https://www.banfacialrecognition.com/map/> (last visited Jan. 27, 2022).

differentiation in the marketplace, serving as a mechanism to cut out the worst offenders.

F. CREATION OF A CERTIFICATION MARKET

Finally, it bears mentioning that the creation of one certification entity potentially can create a market for others.¹⁴⁰ That is, one certification scheme can beget additional ones, especially as industry backs competing schemes with weaker standards, allowing them to continue their current practices but with a claim to ethical certification.¹⁴¹ For example, there are so many eco-labels, of such varying quality, that an entire platform has been created just to help consumers and vendors distinguish between them.¹⁴²

There is no obvious answer to this other than (1) to back a strong scheme with sufficient publicity as to what is meaningful and what is not and (2) to ensure buy-in from a broad set of stakeholders at the outset of creating the regime.

VI. CONCLUSION

This Report has weighed the merits and challenges of a certification regime. At this point a reader may feel the issues are very complicated and that making such a regime work would be a difficult task. We don't disagree. For example, it would be difficult for a certification entity to keep up with the rapid pace of change, especially in the context of machine learning technologies that constantly evolve in the field. The very purpose of this study was to present a set of arguments and considerations for outside consumption.

It may be worth stepping away from the trees, however, to look back at the forest. What is it that certification can accomplish, and what must be avoided?

For certain, certification should not function as a permission structure for simply acquiring new technologies. We do not want agencies or policymakers to co-opt certification as a seal of approval or as a means to dodge criticism from concerned citizens. This is the single greatest concern expressed by the many privacy and civil rights advocates we interviewed. For tech certification to be viable, this concern must be addressed fully.

Similarly, the goal of certification is not to make hard choices for communities and policymakers but to give them the tools to make those

140. See Fromer, *supra* note 108, at 167.

141. See *id.*; GREENPEACE, *supra* note 112, at 9.

142. See *About*, ECOLABEL INDEX, <http://www.ecolabelindex.com/about/> (last visited Jan. 27, 2022).

choices themselves. As we have said, communities have different needs and values, and a commitment to the notion of policing as a democratic enterprise requires honoring those differences.

The hope is that certification might, rather than displacing community choice, facilitate it, while proving a trusted informational voice in decision-making. From our research and discussions, there emerged one universal revelation: there is a crying need for more information about these technologies and an impartial source to provide it. Certification is one way to meet this need, and in doing so, it might help all stakeholders make better decisions and come to an informed consensus—to know the right questions to ask to, and demands to make of, their policing agencies. One hopes policymakers would use certification not as a rationale for a decision already made but as a tool to gather and interpret all of the relevant facts so that they can reach informed conclusions. One hopes that it would lead vendors to compete to out-innovate each other on privacy protections, on transparency, or on mitigating bias.

This is, to be sure, a tall and optimistic order. But it is a far better vision of policing technology than what exists today. It is unclear whether certification ultimately is deemed a valuable approach—although many stakeholders expressed agreement that there is a pressing need for more objective information about policing technology. However, what is clear is that the status quo is unacceptable.

A USER’S GUIDE TO SECTION 230, AND A LEGISLATOR’S GUIDE TO AMENDING IT (OR NOT)

Jeff Kosseff[†]

ABSTRACT

Section 230 of the Communications Decency Act, which immunizes online service providers from liability for user content, is key to the business models of some of the nation’s largest online platforms. For two decades, the 1996 statute was mostly unknown outside of technology law circles. This has changed in recent years, as large social media companies have played an increasingly central role in American life and have thus faced unprecedented scrutiny for their decisions to allow or remove controversial user content. Section 230 has entered the national spotlight as a topic of national media coverage, congressional hearings, and presidential campaign rallies. Unfortunately, not all this attention has accurately portrayed why Congress passed § 230 or how the statute works. The misunderstandings of the law are particularly troubling as Congress is considering dozens of proposals to amend or repeal it. This Article attempts to set the record straight and provide a “user’s guide” to the statute, along with principles for legislators to consider as they evaluate amendments to this vital law.

TABLE OF CONTENTS

I.	INTRODUCTION	758
II.	WHY CONGRESS PASSED § 230.....	761
	A. LIABILITY FOR DISTRIBUTORS BEFORE § 230	761
	B. WHAT § 230 ACTUALLY SAYS.....	768
III.	HOW § 230 WORKS.....	773
	A. THE BROAD SCOPE OF § 230(C)(1).....	773
	B. WORKING AROUND § 230(C)(1)	779
	1. <i>Development or Creation of Content</i>	780
	2. <i>Treatment as Publisher or Speaker</i>	782
	C. JUDICIAL CALLS FOR § 230 REFORM.....	785
IV.	PRINCIPLES FOR § 230 REFORM	788

DOI: <https://doi.org/10.15779/Z38VT1GQ97>

© 2022 Jeff Kosseff.

[†] Associate Professor, Cyber Science Department, United States Naval Academy. The views in this Article are only the author’s and do not represent the Naval Academy, Department of Navy, or Department of Defense.

A.	ELIMINATING § 230 WON'T ELIMINATE THE FIRST AMENDMENT ..	789
B.	§ 230 PROVIDES CERTAINTY TO PLATFORMS.....	791
C.	§ 230 CARVEOUTS CAN HAVE SWEEPING IMPACTS.....	793
D.	“NEUTRALITY” IS ELUSIVE	795
E.	TRANSPARENCY COULD IMPROVE THE § 230 DEBATE.....	798
V.	CONCLUSION	801

I. INTRODUCTION

In 2004, Orin Kerr undertook the vital but unenviable task of explaining the Stored Communications Act to the world. Earlier that year, the Ninth Circuit had issued an opinion that radically broke from previous judicial interpretations of the law, which governs service providers’ disclosure of customers’ emails and other communications records.¹ The Court had interpreted the statute in a way that expanded the types of communications to which it applied, using questionable analysis of key terms in the law. As Kerr observed, the misunderstandings of the Stored Communications Act were pervasive. “Despite its obvious importance, the statute remains poorly understood,” Kerr wrote. “Courts, legislators, and even legal scholars have had a very hard time making sense of the SCA.”²

Kerr’s article, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, has the primary goal of explaining “the basic structure and text of the Act so that legislators, courts, academics, and students can understand how it works—and in some cases, how it doesn’t work.” He also analyzes “how Congress should amend the statute in the future.”³

The article has achieved its purpose—in the eighteen years since its publication, dozens of judges have relied on Kerr’s article to help them interpret the Stored Communications Act’s murky provisions, including in some of the most important cases in the field.⁴

As I write this article in 2022, I feel the same sense of frustration that Kerr likely experienced, but not about the Stored Communications Act. In 2019, I published a book⁵ about the history of § 230 of the Communications Decency

1. See *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).

2. Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004).

3. *Id.* at 1209.

4. See, e.g., *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008).

5. JEFF KOSSEFF, *THE TWENTY-SIX WORDS THAT CREATED THE INTERNET* (2019).

Act,⁶ the statute that immunizes online platforms for liability arising from a great deal of user content. I argued that § 230 is responsible for the open Internet that Americans know today, as platforms are free to allow—or moderate—user content without fearing company-ending litigation.

Since I published the book, this once-obscure law has been thrust into the national spotlight, with calls to repeal the law from all sides of the political spectrum.⁷ Some argue that large social media platforms have failed to remove harmful user-generated content. Others are upset that the platforms moderate too much speech and allegedly discriminate against particular political viewpoints.⁸

Section 230 has become a proxy for these complaints, even when § 230 is not directly related to the particular problem at hand. Politicians, commentators, scholars, and lobbyists are increasingly calling to amend or repeal § 230.⁹ Although the § 230 debate has been loud, it has not been precise. Politicians and reporters have consistently misunderstood how the statute works and what it protects.¹⁰

6. 47 U.S.C. § 230.

7. See Lauren Feiner, *Biden Wants to Get Rid of Law that Shields Companies Like Facebook From Liability for What Their Users Post*, CNBC (Jan. 17, 2020) (“The bill became law in the mid-1990s to help still-nascent tech firms avoid being bogged down in legal battles. But as tech companies have amassed more power and billions of dollars, many lawmakers across the political spectrum along with Attorney General William Barr, agree that some reforms of the law and its enforcement are likely warranted.”).

8. See Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, 2020 U. CHI. LEGAL F. 45, 46–47 (2020) (“Today, politicians across the ideological spectrum are raising concerns about the leeway provided to content platforms under Section 230. Conservatives claim that Section 230 gives tech companies a license to silence speech based on viewpoint. Liberals criticize Section 230 for giving platforms the freedom to profit from harmful speech and conduct.”).

9. See, e.g., Dean Baker, *Getting Serious About Repealing Section 230*, CTR. FOR ECON. & POL’Y RSCH. (Dec. 18, 2020, 12:00 A.M.), <https://cepr.net/getting-serious-about-repealing-section-230/> (“I have argued that repeal would fundamentally change the structure of the industry, leading to a major downsizing of Facebook, Twitter, and other social media giants. It would also level the playing field between social media platforms and traditional media outlets.”).

10. See Ali Sternburg, *Why Do So Many Section 230 Stories Contain Corrections*, DISRUPTIVE COMPETITION PROJECT (Sept. 3, 2019), <https://www.project-disco.org/innovation/090319-why-do-so-many-section-230-stories-contain-corrections/> (“But for Section 230, online services could be sued by plaintiffs for removing anything from extremist content to pornography to fraudulent schemes. Section 230 also ensures that different services will take different approaches to content moderation. However, the frequency of inaccuracy in articles on this subject happens more often than one would expect for a law that is not that complex.”).

Consider the August 6, 2019, cover of the *New York Times* business section—published with the headline “Why Hate Speech on the Internet is a Never-Ending Problem.” Underneath that headline was the main twenty-six word provision of § 230 that provides immunity to online platforms for third-party content. Below that, the *Times* wrote, “Because this law shields it.” The *Times* soon published a correction for that statement: “An earlier version of this article incorrectly described the law that protects hate speech on the internet. The First Amendment, not Section 230, protects it.” Yet within weeks, a federal judge in New Jersey wrote about “Section 230’s grant of immunity for speech-based harms such as hate speech or libel” and cited the article.¹¹ Less than two years later, the *Times* ran another correction, this time for an article about former President Trump’s lawsuit against social media companies that suspended his account. The article “misidentified the legal provision that lets social media companies remove posts that violate their standards. It is the First Amendment, not Section 230.”¹²

This is a particularly unfortunate time for widespread misunderstandings about the statute. Congress is considering many proposals to amend or repeal § 230.¹³ In 2018, Congress enacted the first-ever substantial amendment to the law, providing an exception for certain sex trafficking- and prostitution-related claims. Unfortunately, the widespread misunderstandings of § 230 may lead Congress to make changes that do not achieve their desired outcomes but instead threaten the freedoms that underpin the open internet that § 230 created in the United States.

Just as Kerr hoped to foster a more precise understanding of the Stored Communications Act, this Article aims to provide judges, the media, members of the public, and Congress with a better understanding of § 230’s purpose, mechanics, and impact. The Article debunks some of the most popular myths about § 230 and concludes by providing legislators with principles to guide the debate about the future of § 230 and content moderation.

Part II of the Article examines why Congress passed § 230 in 1996 and what the law actually says. To understand § 230’s purpose, it is necessary to review the First Amendment and common law protections for traditional

11. Order, *Papataros v. Amazon.com*, Civ. No. 17-9836 (D. N.J. Aug. 26, 2019).

12. Corrections, N.Y. TIMES (July 10, 2021).

13. See Cameron F. Kerry, *Section 230 Reform Deserves Careful and Focused Consideration*, BROOKINGS TECHTANK (May 14, 2021), <https://www.brookings.edu/blog/techtank/2021/05/14/section-230-reform-deserves-careful-and-focused-consideration/> (“[M]any blame Section 230 or seize on it as a vehicle to force changes on platforms. But there is little agreement among political leaders as to what are the real problems are, much less the right solutions. The result is that many proposals to amend or repeal Section 230 fail to appreciate collateral consequences—and would ultimately end up doing more harm than good.”).

distributors of speech, such as bookstores and newsstands. Section 230 helps fill in some gaps and uncertainties in those liability standards while also promoting growth and innovation of the nascent internet.

Part III explains how § 230 works in practice by outlining how courts have broadly interpreted the statute to immunize platforms in many contexts. It also describes how some plaintiffs have successfully circumvented § 230's liability protections.

Part IV charts a path forward, or at least provides principles to guide a path forward. Any changes to § 230 could have immediate and sweeping consequences, as seen after the 2018 sex trafficking amendment that caused many websites to change how they handle user content. Much of the debate has focused on repealing § 230 entirely. This Part explains why repealing § 230 would not necessarily solve many of the most significant problems that people have with social media. It instead outlines considerations to guide legislators as they determine whether and how to change § 230.

II. WHY CONGRESS PASSED § 230

Congress passed § 230 in February 1996, at the dawn of the modern, commercial internet. The statute was intended to fill the gaps in the common law governing the liability of companies that distribute third-party content.¹⁴ These rules were developed through decades of First Amendment cases concerning the liability of offline content distributors such as bookstores and newsstands. Although these legal rules worked relatively well in the pre-internet age, courts struggled to apply them to online services, as the following discussion illustrates.

A. LIABILITY FOR DISTRIBUTORS BEFORE § 230

The most important case in the development of the common law distributor liability regime was *Smith v. California*, a 1959 U.S. Supreme Court opinion. The case involved Eleazar Smith, a Los Angeles bookstore owner who was convicted for selling a book in violation of an ordinance that prohibited booksellers from possessing indecent or obscene books.¹⁵ Smith argued that the ordinance violated the First Amendment because it imposed “absolute” or “strict” liability on bookstore owners, no matter if they had any knowledge of the obscene material.

14. See KOSSEFF, *supra* note 5, at 57–78.

15. *Smith v. California*, 361 U.S. 147, 148 (1959).

The Supreme Court agreed with Smith. Eliminating any requirement for scienter “may tend to work a substantial restriction on the freedom of speech and of the press.”¹⁶ Writing for the majority, Justice William Brennan acknowledged that the First Amendment does not protect obscenity, but he wrote that a strict liability ordinance would reduce the distribution of nonobscene, constitutionally protected books:

By dispensing with any requirement of knowledge of the contents of the book on the part of the seller, the ordinance tends to impose a severe limitation on the public’s access to constitutionally protected matter. For if the bookseller is criminally liable without knowledge of the contents, and the ordinance fulfills its purpose, he will tend to restrict the books he sells to those he has inspected; and thus the State will have imposed a restriction upon the distribution of constitutionally protected as well as obscene literature.¹⁷

Brennan recognized that opponents of the decision would argue that an obscenity statute with a scienter requirement would enable distributors to merely lie about whether they knew of or suspected illegality. But he believed that barrier could be overcome. “Eyewitness testimony of a bookseller’s perusal of a book hardly need be a necessary element in proving his awareness of its contents,” Brennan wrote. “The circumstances may warrant the inference that he was aware of what a book contained, despite his denial.”¹⁸

The Supreme Court explicitly avoided delving too deeply into the precise level of scienter that would satisfy the First Amendment, but it suggested possibilities such as: “whether honest mistake as to whether its contents in fact constituted obscenity need be an excuse; whether there might be circumstances under which the State constitutionally might require that a bookseller investigate further, or might put on him the burden of explaining why he did not, and what such circumstances might be.”¹⁹ The Supreme Court’s holding in *Smith* would later be essential to its 1964 landmark ruling in *New York Times v. Sullivan*, in which it required public officials to demonstrate actual malice in libel lawsuits. “A rule compelling the critic of official conduct to guarantee the truth of all his factual assertions—and to do so on pain of libel judgments virtually unlimited in amount—leads to a comparable ‘self-censorship,’” the Court wrote.²⁰

16. *Id.* at 151.

17. *Id.* at 153.

18. *Id.* at 154.

19. *Id.*

20. *N. Y. Times v. Sullivan*, 376 U.S. 254, 279 (1964).

The Court further refined its holding about distributor liability over the next decade. For instance, in a 1968 case, *Ginsberg v. New York*, the Supreme Court affirmed the constitutionality of a state law that penalized the sale of pornographic materials to minors, providing that the seller had “general knowledge of, or reason to know, or a belief or ground for belief which warrants further inspection or inquiry of both . . . the character and content of any material described herein which is reasonably susceptible of examination by the defendant” and the minor’s age.²¹

Relying on a New York state court opinion that had interpreted the same statute, the Supreme Court interpreted the statute to mean that “only those who are *in some manner aware* of the character of the material they attempt to distribute should be punished. It is not innocent but calculated purveyance of filth which is exorcised.”²² Applying this definition, the Supreme Court held that it satisfied the *Smith v. California* scienter requirement. In other words, the Supreme Court does not necessarily require that an ordinance impose an actual knowledge requirement, but having a “reason to know” of the illegal content might suffice.

The First Amendment’s scienter requirement does not necessarily mean that the distributor must know or have reason to know that the content is illegal. In 1974, the Supreme Court in *Hamling v. United States* affirmed the convictions of criminal defendants for distributing obscene materials via the mail. The statute at issue applied to “[w]hoever knowingly uses the mails for the mailing . . . of anything declared by this section . . . to be nonmailable.”²³ The judge instructed the jury that to find the defendants guilty under this law, the jury must find that the defendants “knew the envelopes and packages containing the subject materials were mailed or placed . . . in Interstate Commerce, and . . . that they had knowledge of the character of the materials,” and that the defendants’ “belief as to the obscenity or non-obscenity of the material is irrelevant.”²⁴ The defendants argued that this instruction fell short of the First Amendment’s scienter requirements and that the prosecution required, “at the very least, proof both of knowledge of the contents of the material and awareness of the obscene character of the material.”²⁵

The Supreme Court disagreed and held that the district court’s instructions met the minimum standards under the First Amendment. “It is constitutionally

21. *Ginsberg v. New York*, 390 US 629, 646 (1968) (emphasis in original).

22. *Id.* at 644.

23. *Hamling v. United States*, 418 U.S. 87, 119 (1974).

24. *Id.* at 119–20.

25. *Id.* at 120.

sufficient that the prosecution show that a defendant had knowledge of the contents of the materials he distributed, and that he knew the character and nature of the materials,” Justice Rehnquist wrote for the Court. “To require proof of a defendant’s knowledge of the legal status of the materials would permit the defendant to avoid prosecution by simply claiming that he had not brushed up on the law.”²⁶

Scienter requirements for distributors extend beyond criminal obscenity cases. The Restatement (Second) of Torts incorporated a scienter requirement for defamation, stating that “one who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character.”²⁷ A comment to that rule states that a distributor “is not liable, if there are no facts or circumstances known to him which would suggest to him, as a reasonable man, that a particular book contains matter which upon inspection, he would recognize as defamatory.”²⁸

The California Court of Appeal applied this rule in 1984 in a dispute involving Kenneth Osmond, the actor who played Eddie Haskell on *Leave it to Beaver*, and a chain of adult book stores. After the show went off the air, Osmond became a police officer in Los Angeles. Osmond learned that a chain of adult book stores, EWAP, was selling a pornographic film whose cover stated that the film’s male star was “John Holmes, who played ‘Little Eddie Haskell’ on the ‘Leave it to Beaver’ show.”²⁹ Osmond was the only actor to play Eddie Haskell; he had never been in pornography. Osmond sued the chain for libel. EWAP moved for summary judgment, arguing in part that the two store executives who ordered merchandise for the stores had not heard of Osmond, nor had they seen the carton that contained the allegedly defamatory claim.³⁰ The state trial court granted EWAP’s summary judgment motion, and the California Court of Appeal affirmed.

Relying on the Restatement and *Smith v. California*, the California Court of Appeal wrote that “in order to find the malice or scienter necessary to hold EWAP liable for disseminating the libelous material, a jury would be required to find that EWAP knew or had reason to know of its defamatory character.”³¹ The court concluded that Osmond had not met that standard. “Since Osmond

26. *Id.* at 123.

27. Restatement (Second) of Torts § 581 (AM. L. INST. 1997).

28. *Id.* at cmt. e.

29. *Osmond v. EWAP*, 153 Cal. App. 3d 842, 847 (Cal. Ct. App. 1984).

30. *Id.* at 848.

31. *Id.* at 854.

did not present any evidence which makes us suspect that EWAP either had knowledge of the libel or was aware of information which imposed a duty to investigate, he did not make a sufficient showing of malice to justify consideration of the issue by the jury," the court wrote.³²

Throughout the 1980s, only a handful of published opinions applied the distributor liability standard in defamation cases, and they articulated a similar rule: the liability of a distributor requires knowledge or reason to know of the defamatory or otherwise illegal content.³³ Distributor liability became a bit trickier to apply to the early 1990s commercial online services industry, which allowed customers to use dial-up modems to connect to bulletin boards and forums. These services, like bookstores, distributed content created by others. But the online services, even at that time, could have tens of thousands of users who each posted many messages a day. How did the distributor liability standards apply to these services?

The first case in which a judge attempted answer this question was *Cubby v. CompuServe* in 1991.³⁴ The plaintiffs sued CompuServe over allegedly defamatory statements that were published in a CompuServe forum a contractor managed for CompuServe.³⁵ A federal judge in the Southern District of New York granted CompuServe's summary judgment motion, applying the distributor liability framework and *Smith v. California* and its progeny.

First, the judge concluded that CompuServe was a distributor that was entitled to the same liability standards as a bookstore:

A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information.³⁶

Had the judge not concluded that CompuServe was a distributor, it may have been just as liable for any defamation as the author of the article. The judge acknowledged that even a distributor such as CompuServe could have some control over the third-party content that it distributes because it can

32. *Id.* at 857.

33. *See, e.g.*, *Spence v. Flynt*, 647 F. Supp. 1266, 1273 (D. Wyo. 1986); *Dworkin v. Hustler*, 611 F. Supp. 781, 787 (D. Wyo. 1985).

34. *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

35. *Id.* at 137.

36. *Id.* at 140.

refuse to carry it: “While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a publication, it will have little or no editorial control over that publication’s contents.”³⁷ But because the judge concluded that CompuServe was a distributor, he ruled in the company’s favor, observing that the plaintiffs failed to produce “specific facts” that CompuServe “knew or had reason to know” about the contents of the forum.³⁸

As Allen S. Hammond observed soon after the *Cubby* decision, editorial control appeared to be a key factor in determining an online service’s liability for third-party content. “The greater the discernable control that the system operator exercised over access and content, the greater its potential liability to users and third parties for damage caused by the information’s content,” Hammond wrote.³⁹

The *Cubby* judge’s comment about “editorial control” ultimately would set the wheels in motion for § 230’s passage. Four years after the *CompuServe* dismissal, a New York state trial judge presided over a defamation lawsuit against CompuServe’s competitor, Prodigy. The case arose from user comments on a Prodigy financial discussion forum. The main distinction between CompuServe and Prodigy is that Prodigy had implemented user content guidelines, automatically screened user posts for offensive terms, and contracted with “Board Leaders” who enforced the user guidelines.⁴⁰

The judge concluded that Prodigy was not a distributor like CompuServe but a publisher that faced the same liability as the comments’ author. Key to the judge’s decision were Prodigy’s attempts to moderate user content and that the company “held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition and expressly likening itself to a newspaper.”⁴¹ Seizing on the distinction from *CompuServe*, the judge reasoned that whether Prodigy was a publisher or distributor hinged on whether the plaintiffs proved that it “exercised sufficient editorial control over its computer bulletin boards to render it a publisher with the same responsibilities as a newspaper.”⁴²

37. *Id.*

38. *Id.* at 141.

39. Allen S. Hammond, *Private Networks, Public Speech: Constitutional Speech Dimensions of Access to Private Networks*, 55 U. PITT. L. REV. 1085, 1117–18 (1994).

40. *Stratton Oakmont v. Prodigy Servs Co.*, No. 31063/94, 1995 WL 323710, at *1 (N. Y. Sup. Ct. May 24, 1995).

41. *Id.* at *2.

42. *Id.* at *3.

The judge found two main differences between CompuServe and Prodigy. “First, Prodigy held itself out to the public and its members as controlling the content of its computer bulletin boards,” the judge wrote. “Second, Prodigy implemented this control through its automatic software screening program, and the Guidelines which Board Leaders are required to enforce.”⁴³

Because Prodigy wanted to “control” user content, the judge ruled, it must assume more liability for that content than a hands-off platform such as CompuServe.

“Presumably Prodigy’s decision to regulate the content of its bulletin boards was in part influenced by its desire to attract a market it perceived to exist consisting of users seeking a ‘family-oriented’ computer service,” the judge wrote. “This decision simply required that to the extent computer networks provide such services, they must also accept the concomitant legal consequences.”⁴⁴

The opinion attracted immediate attention from the media and scholars. In an article published the day after the opinion’s release, the *New York Times* reported that an America Online lawyer “said she hoped that on-line services would not be forced to choose between monitoring bulletin boards and assuming liability for users’ messages.”⁴⁵ Norman Redlich and David R. Lurie wrote shortly after the opinion that the “divergent results” between the *Stratton Oakmont* and *CompuServe* cases “suggest a network operator will undertake substantial liability risks if it chooses to play any role in policing the content of communications on its system.”⁴⁶ Robert Hamilton, who successfully represented CompuServe in its defamation case, wrote that the *Stratton Oakmont* ruling was erroneously based on a dichotomy between “publishers” and “distributors” when, under the common law of libel, “the legal term ‘publisher’ includes both the person who creates the recorded defamatory text and the person who distributes it to others, but only when they have knowledge of the defamatory content that is disseminated.”⁴⁷ In other words, the editorial control that a platform exercises is not what determines whether a distributor is liable; instead, it is whether the distributor knows or has reason to know of the defamatory content.

43. *Id.* at *4.

44. *Id.* at *5.

45. Peter H. Lewis, *Judge Allows Libel Lawsuit Against Prodigy to Proceed*, N.Y. TIMES (May 26, 1995), <https://www.nytimes.com/1995/05/26/business/the-media-business-judge-allows-libel-lawsuit-against-prodigy-to-proceed.html>.

46. Norman Redlich & David R. Lurie, *First Amendment Issues Presented by the Information Superhighway*, 25 SETON HALL L. REV. 1446, 1458 (1994-1995).

47. Robert W. Hamilton, *Liability for Third-Party Content on the Internet*, 8 SETON HALL CONST. L. J. 733, 734 n.2 (1998).

In 1995, *Cubby* and *Stratton Oakmont* were the only U.S. court opinions that examined the liability of online services for the user content they distributed. Although these rulings were not binding on other courts, they were the only opinions that other judges could look to for guidance. And they suggested that platforms received greater liability protection if they took a hands-off approach to user content.

B. WHAT § 230 ACTUALLY SAYS

Congress was paying close attention in 1995 as it drafted the first overhaul of federal telecommunications laws in six decades. The new commercial internet was not the primary focus of the debate, with one significant exception. Members of Congress were concerned about the availability of pornography to minors who were accessing the internet from home, school, and libraries.⁴⁸ The July 3, 1995, cover of *Time* depicted a shocked child illuminated behind a keyboard, with the headline “Cyberporn.”⁴⁹

To address this problem, Senator J. James Exon managed to add the Communications Decency Act (CDA) to the Senate’s version of the Telecommunications Act. The CDA would have imposed criminal penalties for the online transmission of indecent material to minors.⁵⁰ House members, however, had significant concerns about the constitutionality of the Act. House Speaker Newt Gingrich, at the time, stated that Exon’s bill was “clearly a violation of free speech and it’s a violation of the right of adults to communicate with each other.”⁵¹

Representatives Chris Cox and Ron Wyden took the lead in developing another way to help to reduce minors’ access to online pornography while also fostering the growth of the nascent commercial internet. They also sought to reverse the *Stratton Oakmont* decision,⁵² which they saw as creating a perverse incentive for platforms to take an entirely hands-off approach to user content.

Representatives Cox and Wyden introduced the Internet Freedom and Family Empowerment Act⁵³ on June 30, 1995, a little over a month after the *Stratton Oakmont* decision. With some changes, the Act would eventually

48. See KOSSEFF, *supra* note 5, at 61-62.

49. TIME, July 3, 1995.

50. 141 Cong. Rec. S16006-07 (daily ed. 14, 1995) (statement of Sen. Exon).

51. Tim Murphy, *How Newt Gingrich Saved Porn*, MOTHER JONES (Dec. 2, 2011) <https://www.motherjones.com/politics/2011/12/how-newt-gingrich-saved-porn/>.

52. *Stratton Oakmont v. Prodigy Servs. Co.*, No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1995).

53. H.R. 1978, 104th Cong. (1995).

become what is now known as § 230.⁵⁴ The Act has two primary provisions, which at first were in the same paragraph, but throughout the legislative process were broken out into § 230 (c)(1) and § 230 (c)(2).

Section (c)(1) contains what I refer to as the twenty-six words that created the internet: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”⁵⁵ The Act broadly defines “interactive computer service” to mean “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.”⁵⁶ Section 230 defines “information content provider” as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.”⁵⁷

As described in Part II, courts would soon interpret § 230(c)(1) to mean that platforms are not responsible for the content that their users post, whether or not they moderated user content. This would remove the specter of increased liability for platforms that exercise “editorial control,” as in *Stratton Oakmont*. Section 230(c)(1) only applies to information “that was “provided by another information content provider.” Thus, if the platform is “responsible, in whole or in part” for creating or developing content, § 230(c)(1) would not apply.

Section 230(c)(2) provides further protection for moderation, as well as for providing tools, such as website blockers, that allow users to control harmful content. The provision states that interactive computer service providers cannot be liable due to “any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected”⁵⁸ or enabling or providing “the technical means to restrict access” to such material.⁵⁹

54. Unless otherwise noted, this Article quotes from the codified version of §230 rather than the introduced bill.

55. 47 U.S.C. § 230(c)(1).

56. 47 U.S.C. § 230(f)(2).

57. 47 U.S.C. § 230(f)(3).

58. 47 U.S.C. § 230(c)(2)(A).

59. 47 U.S.C. § 230(c)(2)(B).

Section 230 has exceptions for the enforcement of federal criminal law,⁶⁰ intellectual property law,⁶¹ and electronic communications privacy laws.⁶² The intellectual property law exception is particularly important to keep in mind, as some media coverage has incorrectly stated that § 230 protects platforms from copyright infringement claims.⁶³ (It is actually the Digital Millennium Copyright Act, an entirely different law, that sets the framework for platform liability arising from users' copyright infringement.)⁶⁴

Section 230 does not exempt state criminal laws, though in 2018, Congress amended the law to create an exception for certain state criminal prosecutions involving sex trafficking and prostitution as well as some federal civil actions involving sex trafficking.⁶⁵

Section 230 as introduced also prohibited the FCC from having authority over “economic or content regulation of the Internet or other interactive computer services.”⁶⁶ That provision would not remain in the final bill after conference committee, but it illustrated Representatives Cox and Wyden’s goal of fostering the internet by removing the threat of government regulation—a very different approach from Senator Exon’s bill.

To clarify their intentions, Representatives Cox and Wyden included statements of findings and policy in § 230. Among the findings of § 230 was that the “services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops”⁶⁷ and that they “offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.”⁶⁸ In line with the hands-off approach to the internet, § 230 includes a finding that online services “have flourished, to the benefit of all Americans, with a minimum of government regulation.”⁶⁹

Section 230’s policy statement reflects similar goals for an unregulated internet that relies on the platforms to help users block objectionable content. Among the policies are “to promote the continued development of the

60. 47 U.S.C. § 230(e)(1).

61. 47 U.S.C. § 230(e)(2).

62. 47 U.S.C. § 230(e)(4).

63. See Mike Masnick, *NY Times Publishes A Second, Blatantly Incorrect, Trashing Of Section 230, A Day After Its First Incorrect Article*, TECHDIRT (Aug. 13, 2019).

64. 17 U.S.C. § 512.

65. 47 U.S.C. § 230(e)(5).

66. H.R. 1978, 104th Cong. § d (1995).

67. 47 U.S.C. § 230(a)(2).

68. 47 U.S.C. § 230(a)(3).

69. 47 U.S.C. § 230(a)(4).

Internet and other interactive computer services and other interactive media”;⁷⁰ “to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services”;⁷¹ and “to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.”⁷²

Many of these findings and policy statements came from a 1995 report coordinated by the Center for Democracy and Technology, which urged “user empowerment” by providing parents with tools such as Net Nanny to block inappropriate online content.⁷³ The report highlighted the unconstitutionality of criminalizing indecent content, and it noted that the online services industry “is committed to developing more and better solutions, and the open nature of the Internet provides a wealth of possibilities for parental empowerment tools that may not yet have been imagined.”⁷⁴

With this history in mind, it is important to point out that § 230 was intended to provide platforms with the flexibility to determine when and how to moderate user content. As discussed in Part III, some participants in the current debate about § 230 have incorrectly suggested that it only applies to “neutral platforms.” To the contrary, Congress wanted to pass a law to overturn *Stratton Oakmont* and ensure that platforms did *not* have an incentive to be neutral.

This goal was clear when the bill came up for House floor debate on August 4, 1995, as an amendment to the House’s version of the telecommunications overhaul. Representative Cox emphasized the “backward” nature of the *Stratton Oakmont* ruling and argued the bill would:

[P]rotect computer Good Samaritans, online service providers, anyone who provides a front end to the Internet, let us say, who takes steps to screen indecency and offensive material for their customers. It will protect them from taking on liability such as occurred in the Prodigy case in New York that they should not face for helping us and for helping us solve this problem.⁷⁵

70. 47 U.S.C. § 230(b)(1).

71. 47 U.S.C. § 230(b)(3).

72. 47 U.S.C. § 230(b)(2).

73. INTERACTIVE WORKING GROUP REPORT, PARENTAL EMPOWERMENT, CHILD PROTECTION, AND FREE SPEECH IN INTERACTIVE MEDIA (1995).

74. *Id.*

75. 104 Cong. Rec. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).

But Representative Cox also articulated a second goal:

[To] establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet, that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the Internet because frankly the Internet has grown up to be what it is without that kind of help from the Government.⁷⁶

Representative Robert Goodlatte emphasized the impracticality of holding service providers liable for all of their user content:

There is no way that any of those entities, like Prodigy, can take the responsibility to edit out information that is going to be coming into them from all manner of sources onto their bulletin board. We are talking about something that is far larger than our daily newspaper. We are talking about something that is going to be thousands of pages of information every day, and to have that imposition imposed on them is wrong.⁷⁷

The Cox-Wyden amendment was positioned as the alternative to Senator Exon's Communications Decency Act. Representative Zoe Lofgren spoke in favor of the Cox-Wyden amendment, arguing that Exon's bill "is like saying that the mailman is going to be liable when he delivers a plain brown envelope for what is inside it."⁷⁸

The House voted 420-4 to add § 230 to its telecommunications reform bill.⁷⁹ Both the Senate's Communications Decency Act and Cox and Wyden's § 230 were included in the final, negotiated telecommunications bill signed into law in February 1996.

Perhaps § 230's prohibition on FCC regulation of internet content was removed from the final bill because it might have conflicted with the Communications Decency Act, but there is no record as to the reasoning for that change. The conference committee did, however, write in the conference report that it intended to overrule *Stratton Oakmont* "and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material."⁸⁰ To clarify Section 230's impact on litigation, the enacted law contains a provision that was not in the introduced bill, stating

76. *Id.*

77. *Id.* at H8471.

78. *Id.*

79. *Id.* at H8478.

80. H. R. Rep. No. 104-458, at 194 (1996).

that “[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.”⁸¹

Because § 230 was placed in the same part of the telecommunications law as the Communications Decency Act, it became known as § 230 of the Communications Decency Act, even though it would be more accurate to call the provision § 230 of the Communications Act of 1934.⁸² A year later, the Supreme Court struck down as unconstitutional the Senate’s Communications Decency Act, which penalized the transmission of indecent materials.⁸³ But the opinion did not affect § 230, as it did not involve imposing penalties for the distribution of constitutionally protected speech.

III. HOW § 230 WORKS

When Congress passed § 230, the liability protections of § 230(c)(1) and § 230(c)(2) received little public attention. Most of the media attention focused on Exon’s Communications Decency Act, and the Telecommunications Act of 1996 was portrayed as a loss for civil liberties advocates and technology companies.⁸⁴ The lack of attention to § 230 likely was at least partly because it was unclear how courts would interpret the statute. It would take another year for courts to determine that § 230(c)(1) provides platforms with extraordinarily broad protections.

A. THE BROAD SCOPE OF § 230(C)(1)

There are at least two ways to read the twenty-six words of § 230(c)(1). A limited reading would conclude that prohibiting interactive computer service providers from being “treated” as publishers or speakers of third-party content means that all such providers are instead treated as distributors.⁸⁵ Under that

81. 47 U.S.C. § 230(e).

82. For an exhaustive discussion of § 230’s name, see Blake Reid, *Section 230 of . . . What?* (Sept. 4, 2020), <https://blakereid.org/section-230-of-what/>.

83. *Reno v. American Civil Liberties Union*, 521 U.S. 844, 885 (1997) (“The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it.”).

84. See Howard Bryant & David Plotnikoff, *How the Decency Fight Was Won*, SAN JOSE MERCURY NEWS (Mar. 3, 1996) (stating that the “Internet’s free speech supporters lost their historic battle over cyberspace decency standards because they were outgunned, outflanked, out-connected and out-thought in the most crucial battle of the online community’s brief history”).

85. See Ian Ballon, *Zeran v. AOL: Why the Fourth Circuit Is Wrong*, J. INTERNET L. (1998) (“In this author’s view, Congress effectively codified an altered version of the *Cubby* standard

reading, a platform would be liable for user content if it knew or had reason to know of the defamatory or otherwise illegal content. In other words, if a platform received a complaint alleging that user content was defamatory, the platform would either need to take down the content or defend a defamation suit just as the author would. A platform also might be liable even without having received a complaint, though the lack of on-point caselaw makes it difficult to predict how a court would determine when a platform had a “reason to know” of the content.

A second, broader, reading would interpret § 230(c)(1) as barring any claim against an interactive computer service provider arising from third-party content unless an exception applied. This would mean that even if a platform knew or had reason to know of defamatory user content, it would not be liable for that content. Such a reading would require a court to conclude that treating a platform as a distributor would fall under § 230’s prohibition of treatment as a publisher. In other words, the broader interpretation of § 230 requires courts to consider a distributor as a type of publisher.

The first federal appellate court to interpret § 230(c)(1) adopted the broader reading. On November 12, 1997, the Fourth Circuit issued its opinion in *Zeran v. America Online*. The case involved offensive posts on an AOL bulletin board that purported to sell t-shirts with tasteless jokes about the recent Oklahoma City bombing. The posts instructed readers to call “Ken” at a Seattle phone number that belonged to Ken Zeran.⁸⁶ Zeran, who had nothing to do with the advertisements and did not even have an AOL account, received many angry calls and death threats.⁸⁷ Zeran repeatedly contacted AOL about the ads, but the company failed to promptly remove them or prevent their reposting.⁸⁸

Zeran sued AOL for negligence. The common law and First Amendment defense for distributors likely would not have succeeded for AOL, as Zeran’s claims arose from AOL’s failure to remove and prevent the postings *after* he informed the company of them. Thus, AOL defended itself on the basis that § 230 immunized it from Zeran’s lawsuit. But the only way that this defense would work is if the court agreed with the broader interpretation of § 230: that

under which a service provider (or user) may be held indirectly liable for third party acts of defamation only in instances where it actually knew that material posed online was defamatory and failed to take any action, or in very limited circumstances where it failed to act despite reason to know that material was defamatory (provided that the basis for imputed knowledge is not the provider’s acts of monitoring online content).”).

86. *Zeran v. America Online*, 129 F.3d 327, 329 (4th Cir. 1997).

87. *Id.*

88. *Id.*

it not only prevented interactive computer service provider from being treated as publishers but also as distributors.

The district court agreed with AOL's broad reading of § 230 and dismissed the case, writing that "distributor liability, or more precisely, liability for knowingly or negligently distributing defamatory material, is merely a species or type of liability for publishing defamatory material."⁸⁹ Zeran appealed, and the Fourth Circuit affirmed the dismissal and the broad reading of §230's liability protections.

Writing for the unanimous three-judge panel, Judge J. Harvie Wilkinson observed that Congress passed § 230 to foster open and free discourse on the internet:

Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.⁹⁰

Wilkinson agreed with the district court that § 230 precludes notice-based liability for distributors. "The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law," Wilkinson wrote. "To the contrary, once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher."⁹¹

Wilkinson also recognized the burdens on free speech that distributor liability would create and wrote that such a chilling effect would conflict with § 230's purpose: "If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message." According to Wilkinson, "Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information."⁹²

89. Zeran v. America Online, 958 F. Supp. 1124, 1133 (E.D. Va. 1997).

90. Zeran v. America Online, 129 F.3d 327, 330 (4th Cir. 1997).

91. *Id.* at 332.

92. *Id.* at 333.

Allowing platforms to become liable upon notice, Wilkinson wrote, would allow plaintiffs to effectively veto online speech that they want removed from the internet.⁹³ Congress, he wrote, did not intend such an outcome. “Whenever one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply ‘notify’ the relevant service provider, claiming the information to be legally defamatory,” Wilkinson wrote. “In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability.” Wilkinson read § 230(c)(1) as immunizing platforms for a wide range of activities that publishers perform, including “deciding whether to publish, withdraw, postpone or alter content.”⁹⁴

Wilkinson’s ruling soon attracted some criticism from scholars who argued that Congress only intended to impose distributor liability; it did not intend an absolute bar to liability even if the platforms knew or had reason to know of the defamatory or illegal content.⁹⁵

With no other guidance from federal appellate courts, judges nationwide soon adopted Wilkinson’s broad reading of § 230. For instance, in 1998, Judge Paul Friedman of the U.S. District Court for the District of Columbia dismissed a lawsuit against AOL for an allegedly defamatory Matt Drudge column that AOL distributed. The plaintiff argued that § 230 did not apply. Quoting extensively from Wilkinson’s opinion, Friedman wrote that the “court

93. *Id.* at 330.

94. *Id.*

95. See, e.g., David R. Sheridan, *Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act Upon Liability for Defamation on the Internet*, 61 ALB. L. REV. 147, 151 (1997) (writing of the district court’s dismissal in the *Zeran* case: “It can be argued that the *Zeran* holding is supported neither by the text of the law nor by the legislative history expressing an intent to overrule *Stratton Oakmont*. However, the *Zeran* holding is arguably consistent with Congress’s intent, expressed in the CDA itself, to put control over content in the hands of users of interactive computer services and of parents of minor users.”); Todd G. Hartman, *Marketplace vs. the Ideas: The First Amendment Challenges to Internet Commerce*, 12 HARV. J. L. & TECH. 419, 446-47 (1999) (“Thus, despite clear legal precedent arguing for a narrow interpretation of section 230, the court extended the scope of section 230 to provide AOL immunity from distributor liability as well as publisher liability. In doing so, the *Zeran* court ignored the specific intent of Congress in passing section 230, which was to facilitate the restriction of offensive material, not restrict its dissemination.”). *Contra* Cecilia Ziniti, *Optimal Liability System for Online Service Providers: How Zeran v. America Online Got It Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583 (2008) (highlighting the chilling effects of a distributor liability system and arguing that “*Zeran* has proven efficient and adaptable and nurtured the growth of beneficial innovation online”).

in *Zeran* has provided a complete answer to plaintiffs' primary argument, an answer grounded in the statutory language and intent of Section 230."⁹⁶ Likewise, in 2000, the Tenth Circuit affirmed the dismissal of a lawsuit against AOL for distributing allegedly inaccurate stock information, citing *Zeran* for the proposition that "Congress clearly enacted § 230 to forbid the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions."⁹⁷ As Eric Goldman wrote in 2017, *Zeran* is "the most important Section 230 ruling to date-and probably the most important court ruling in Internet Law."⁹⁸

Although the floor debate about § 230 did not directly address whether Congress intended the broad reading that Wilkinson applied, it is noteworthy that in a report accompanying a 2002 children's online safety law, the House Committee on Energy and Commerce, citing *Zeran* and other early opinions that relied on its reasoning, wrote that "[t]he courts have correctly interpreted section 230(c), which was aimed at protecting against liability for such claims as negligence."⁹⁹ Likewise, both Representatives Cox and Wyden have said that the *Zeran* interpretation was correct.¹⁰⁰

Under the *Zeran* rule, as interpreted by other courts, even platforms that encourage users to post scurrilous content receive § 230 protections. For instance, in *Jones v. Dirty World Entertainment Recordings*, a website called TheDirty.com invited users to provide "dirt" on others via a submission form that said, "Tell us what's happening. Remember to tell us who, what, when, where, why."¹⁰¹ The website's staff selected about 150 to 200 of the thousands of daily submissions for posting, and they all were signed "THE DIRTY ARMY."¹⁰² The site's operator, Nik Richie, often added a short humorous comment beneath the user submission.¹⁰³ TheDirty users posted a number of submissions about Sarah Jones, a high school teacher and NFL cheerleader, including allegations that she slept with football players and had a sexually

96. *Blumenthal v. Drudge*, 992 F. Supp. 44, 51 (D.D.C. 1998).

97. *Ben Ezra, Weinstein, & Co. v. America Online*, 206 F.3d 980, 986 (10th Cir. 2000).

98. Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 TUL. J. TECH. & INTELL. PROP. 1, 3 (2017).

99. H.R. Rep. No. 107-449, at 13 (2002).

100. See KOSSEFF, *supra* note 5, at 95; Brief for Chris Cox, Former Member of Congress and Co-Author of CDA Section 230, and Netchoice as *Amici Curiae* Supporting Defendants and Affirmance at 23, *La Park La Break LLC v. Airbnb, Inc.*, No. 18-55113 (9th Cir. Sept. 27, 2018).

101. *Jones v. Dirty World Ent. Recordings*, 755 F.3d 398, 402-03 (6th Cir. 2014).

102. *Id.* at 403.

103. *Id.*

transmitted disease.¹⁰⁴ Beneath one of the posts, Richie wrote, “Why are all high school teachers freaks in the sack?”¹⁰⁵ Despite Jones’ repeated pleas, the website refused to remove the posts.¹⁰⁶ She sued the website for defamation, false light, and intentional infliction of emotional distress.¹⁰⁷

The district court refused to dismiss the case under § 230, reasoning that “a website owner who intentionally encourages illegal or actionable third-party postings to which he coadds his own comments ratifying or adopting the posts becomes a ‘creator’ or ‘developer’ of that content and is not entitled to immunity.”¹⁰⁸ The case went to trial and led to a \$338,000 verdict for Jones.¹⁰⁹ But the Sixth Circuit reversed the verdict, holding that § 230 did in fact immunize the website. In line with other circuits, the Sixth Circuit ruled that a website has developed content for the purposes of § 230 if it has made a “material contribution to the alleged illegality of the content,” meaning that it is “responsible for what makes the displayed content allegedly unlawful.”¹¹⁰ Merely encouraging the content, the Sixth Circuit held, was not enough to constitute “development” under § 230:

Many websites not only allow but also actively invite and encourage users to post particular types of content. Some of this content will be unwelcome to others — e.g., unfavorable reviews of consumer products and services, allegations of price gouging, complaints of fraud on consumers, reports of bed bugs, collections of cease-and-desist notices relating to online speech. And much of this content is commented upon by the website operators who make the forum available. Indeed, much of it is “adopted” by website operators, gathered into reports, and republished online. Under an encouragement test of development, these websites would lose the immunity under the CDA and be subject to hecklers’ suits aimed at the publisher.¹¹¹

104. *Id.*

105. *Id.* at 404.

106. *Id.*

107. *Id.* at 405.

108. *Id.* at 409.

109. *Id.* at 405–06.

110. *Id.* at 410.

111. *Id.* at 414.

Jones received substantial media and scholarly attention, with some arguing that § 230 should not protect sites such as *TheDirty*¹¹² and others asserting that the Sixth Circuit correctly interpreted the statute.¹¹³

The vast majority of § 230-related dismissals involve § 230(c)(1), including decisions not only to keep material up but to take material down. In a 2020 review of more than 500 § 230 decisions over two decades, the Internet Association found only nineteen involved § 230(c)(2).¹¹⁴ As the Ninth Circuit wrote in 2009, § 230(c)(1) “shields from liability all publication decisions, whether to edit, to remove, or to post, with respect to content generated entirely by third parties.”¹¹⁵ Section 230(c)(2)’s protections for good-faith actions to remove objectionable content, the court wrote, could apply to interactive computer service providers who are not necessarily covered by § 230(c)(1). “Thus, even those who cannot take advantage of subsection (c)(1), perhaps because they developed, even in part, the content at issue, can take advantage of subsection (c)(2) if they act to restrict access to the content because they consider it obscene or otherwise objectionable,” the Court wrote.¹¹⁶ “Additionally, subsection (c)(2) also protects internet service providers from liability not for publishing or speaking, but rather for actions taken to restrict access to obscene or otherwise objectionable content.”¹¹⁷

B. WORKING AROUND § 230(c)(1)

Courts have imposed some limits on the application of § 230(c)(1)’s broad immunity. Judges have denied § 230(c)(1) protection in two situations: (1) where the platform at least partly developed or created the content; and (2)

112. See Laura Cannon, *Indecent Communications: Revenge Porn and Congressional Intent of Sec. 230(c)*, 90 TUL. L. REV. 471, 490 (2015) (“The Sixth Circuit, commentators, scholars, and interested parties failed to distinguish between websites that solicit user input to gauge services or promote consumer confidence and websites that exist solely to elicit tortious content.”).

113. See Christine N. Walz & Robert L. Rogers II, *Sixth Circuit’s Decision in Jones v. Dirty World Entertainment Recordings LLC Repairs Damage to Communications Decency Act*, 30 COMM. LAW. 4 (2014) (“The Sixth Circuit has therefore not overreached, and has retained adequate remedies for the victims of defamation that more accurately fulfill the congressional intent behind § 230 of the CDA.”).

114. ELIZABETH BANKER, INTERNET ASSOCIATION, A REVIEW OF SECTION 230’S MEANING & APPLICATION BASED ON MORE THAN 500 CASES (July 27, 2020) (“Of these, the vast majority involved disputes over provider efforts to block spam. The remainder were resolved under Section 230(c)(1), Anti-SLAPP motions, the First Amendment, or for failure to state a claim based on other deficiencies.”).

115. *Barnes v. Yahoo! Inc.*, 570 F.3d 1096, 1105 (9th Cir. 2009).

116. *Id.* (internal citations omitted).

117. *Id.* (internal citations omitted).

where the claim did not treat the platform as the publisher or speaker of third-party content.

1. *Development or Creation of Content*

Section 230(c)(1) only applies to information provided by *another* information content provider, which the statute defines as a person or entity “that is responsible, in whole or in part, for the creation or development of information.”¹¹⁸ Thus, if the platform itself is even partly responsible for creating or developing content, it cannot claim § 230 protections for that content.

In perhaps the most influential opinion to narrow some of § 230’s protections, the Ninth Circuit, sitting en banc in 2008, partly refused to immunize a roommate-matching website, Roommates.com, for alleged violations of federal and state housing laws. The alleged violations arose from Roommates.com’s user-registration process, which required users to complete a questionnaire for users to provide demographic information, such as sexual orientation and sex, and indicate their preferences from a list of demographic categories.¹¹⁹

The Ninth Circuit ruled that § 230 did not apply to claims arising from any allegedly discriminatory questions that the websites asked. “The CDA does not grant immunity for inducing third parties to express illegal preferences. Roommate’s own acts—posting the questionnaire and requiring answers to it—are entirely its doing and thus § 230 of the CDA does not apply to them,” the Court wrote.¹²⁰ The majority reasoned that if a real estate broker is prohibited from asking about a prospective buyer’s race, an online platform faces that same prohibition.¹²¹

Likewise, the Ninth Circuit concluded that § 230 did not immunize the website from claims arising from the “development and display of subscribers’ discriminatory preferences.”¹²² The court reasoned that this allegedly discriminatory content comes directly from the mandatory registration process. “By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated

118. 47 U.S.C. 230(f)(3).

119. *Fair Hous. Council of San Fernando Valley v. Roommates.com*, 521 F.3d 1157, 1161-62 (9th Cir. 2008) (en banc).

120. *Id.* at 1165.

121. *Id.* at 1164 (“If such questions are unlawful when posed face-to-face or by telephone, they don’t magically become lawful when asked electronically online. The Communications Decency Act was not meant to create a lawless no-man’s-land on the Internet.”).

122. *Id.*

answers, Roommate [sic] becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information,” the Court wrote.¹²³

But the Ninth Circuit did not entirely deny § 230 protection to Roommates.com. The Court held that § 230 applied to any allegedly discriminatory statements in the freeform “Additional Comments” section of user profiles. “The fact that Roommate [sic] encourages subscribers to provide something in response to the prompt is not enough to make it a ‘develop[er]’ of the information under the common-sense interpretation of the term we adopt today,” the Court wrote.¹²⁴

“It is entirely consistent with Roommate’s [sic] business model to have subscribers disclose as much about themselves and their preferences as they are willing to provide,” the Court added.¹²⁵ “But Roommate [sic] does not tell subscribers what kind of information they should or must include as ‘Additional Comments,’ and certainly does not encourage or enhance any discriminatory content created by users.”¹²⁶

As the majority summarized in *Roommates.com*, “a website helps to develop unlawful content, and thus falls within the exception to § 230, if it contributes materially to the alleged illegality of the content.”¹²⁷ Dissenting, Judge McKeown wrote that the majority misinterpreted § 230. “The plain language and structure of the CDA unambiguously demonstrate that Congress intended these activities—the collection, organizing, analyzing, searching, and transmitting of third-party content—to be beyond the scope of traditional publisher liability,” the judge wrote. “The majority’s decision, which sets us apart from five circuits, contravenes congressional intent and violates the spirit and serendipity of the Internet.”¹²⁸

Still, other courts adopted the majority’s narrower reading of § 230. The next year, the Tenth Circuit adopted the material contribution test and concluded that § 230 did not protect the operator of a website from a Federal Trade Commission lawsuit alleging that third-party researchers used the

123. *Id.* at 1166.

124. *Id.* at 1172.

125. *Id.* at 1174.

126. *Id.*

127. *Id.* at 1168.

128. *Id.* at 1177 (McKeown, J., concurring in part and dissenting in part).

website to provide consumers with material that allegedly violated privacy laws.¹²⁹

Roommates.com is one of the most cited § 230 opinions and was the first clear recognition that courts would restrict § 230.¹³⁰ But in more than a decade since the opinion, other courts have used its reasoning relatively sparingly to deny § 230 protections. As Eric Goldman observed, “most courts have read *Roommates.com*’s exception to Section 230 fairly narrowly.”¹³¹

2. *Treatment as Publisher or Speaker*

Some courts have also concluded that § 230 does not apply because the lawsuits do not seek to treat the interactive computer service providers as publishers or speakers of third-party content.

This § 230 workaround was first prominently displayed in a 2009 Ninth Circuit case, *Barnes v. Yahoo*. The plaintiff’s ex-boyfriend allegedly posted explicit images of her on a Yahoo dating website, also listing her contact information.¹³² This caused men to visit and contact her at work, seeking sex.¹³³ The plaintiff complied with Yahoo’s intricate complaint process to have the profile removed, but the company did not respond.¹³⁴ After a local television show began to prepare a story about the plaintiff’s situation, a Yahoo executive told the plaintiff to fax them the necessary information and they would “personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it.”¹³⁵ The plaintiff faxed the

129. See *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1200 (10th Cir. 2009) (“By paying its researchers to acquire telephone records, knowing that the confidentiality of the records was protected by law, it contributed mightily to the unlawful conduct of its researchers. Indeed, Accusearch’s responsibility is more pronounced than that of *Roommates.com*. *Roommates.com* may have encouraged users to post offending content; but the offensive postings were Accusearch’s *raison d’etre* and it affirmatively solicited them.”).

130. See Mary Graw Leary, *The Indecency and Injustice of Section 230 of the Communications Decency Act*, 41 HARV. J. L. & PUB. POL’Y 553, 576 (2018) (“[H]olding that *Roommates.com* was a content provider made it one of the few cases to find potential liability for a website. In so doing it recognized a website could be both an interactive computer service as well as a content provider, at least where the website helped to develop the information . . .”).

131. Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 TUL. J. TECH. & INTELL. PROP. 1, 4 (2017) (“The opinion emphatically says the following: ‘If you don’t encourage illegal content, or design your website to require users to input illegal content, you will be immune.’ Perhaps surprisingly, many courts have cited this *Roommates.com* language while ruling in favor of Section 230 immunity.”).

132. *Barnes v. Yahoo! Inc.*, 570 F.3d 1096, 1098 (9th Cir. 2009).

133. *Id.*

134. *Id.*

135. *Id.* at 1099.

necessary information, but she did not hear back from Yahoo. Two months later, she sued Yahoo for negligent undertaking and promissory estoppel.¹³⁶ The district court dismissed the entire lawsuit under § 230.¹³⁷

On appeal, the Ninth Circuit affirmed the § 230-based dismissal of the negligent undertaking claim.¹³⁸ But the Ninth Circuit reversed the dismissal of the promissory estoppel claim, reasoning that the plaintiff “d[id] not seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promisor who has breached.”¹³⁹ Making a promise, the Court wrote, “is different because it is not synonymous with the performance of the action promised. That is, whereas one cannot undertake to do something without simultaneously doing it, one can, and often does, promise to do something without actually doing it at the same time.”¹⁴⁰

In other words, § 230 did not protect Yahoo from a promissory estoppel claim because the success of the claim did not require Yahoo to be treated as the publisher or speaker of third-party content. This is different from the *Roommates.com* reasoning, which avoids § 230 protections due to the platform’s material contribution to the creation of the illegality.

More recently, in 2016, the Ninth Circuit reversed the § 230 dismissal of a lawsuit against Internet Brands, the operator of a modeling website. The site enabled models to post profiles for talent scouts.¹⁴¹ The plaintiff was contacted by a man, purporting to be a talent scout, who later drugged and raped her with another man.¹⁴² The plaintiff, Jane Doe, alleged that Internet Brands had known about the two men previously using the site to identify women who they would later rape.¹⁴³

The Ninth Circuit reversed the district court’s § 230 dismissal of the case, reasoning that Jane Doe’s lawsuit did not treat Internet Brands as the publisher or speaker of third-party content. The plaintiff was not seeking to hold

136. *Id.*

137. *Id.*

138. *Id.* at 1103 (“In other words, the duty that Barnes claims Yahoo violated derives from Yahoo’s conduct as a publisher—the steps it allegedly took, but later supposedly abandoned, to de-publish the offensive profiles. It is because such conduct is publishing conduct that we have insisted that section 230 protects from liability any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online.”) (internal quotation marks and citation omitted).

139. *Id.* at 1107.

140. *Id.*

141. *Doe v. Internet Brands*, 824 F.3d 846, 848 (9th Cir. 2016).

142. *Id.* at 849.

143. *Id.*

Internet Brands liable for the profile that she posted, nor did her lawsuit allege that the men had posted content on the site, the Court noted.¹⁴⁴

“Instead, Jane Doe attempts to hold Internet Brands liable for failing to warn her about information it obtained from an outside source about how third parties targeted and lured victims through Model Mayhem,” the Court wrote. “The duty to warn allegedly imposed by California law would not require Internet Brands to remove any user content or otherwise affect how it publishes or monitors such content.”¹⁴⁵

The Ninth Circuit extended this somewhat more limited reading of § 230 in *Lemmon v. Snap*.¹⁴⁶ The plaintiffs were parents of two teenagers who died in a car accident. They alleged that their sons were using a Snapchat function known as “Speed Filter,” which allows users to take photos or videos while recording the speed at which they are traveling.¹⁴⁷ Many Snapchat users allegedly played a game in which they tried to record a speed at 100 miles per hour or greater. The plaintiffs’ sons were traveling at up to 123 miles per hour before their car crashed.¹⁴⁸

The parents sued Snap for negligent design, but the district court dismissed the case based on § 230. The Ninth Circuit reversed the dismissal, reasoning that the lawsuit did not treat Snap as the publisher or speaker of third-party content. “To the extent Snap maintains that CDA immunity is appropriate because the Parents’ claim depends on the ability of Snapchat’s users to use Snapchat to communicate their speed to others, it disregards our decision in *Internet Brands*,” the Ninth Circuit wrote. “That Snap allows its users to transmit user-generated content to one another does not detract from the fact that the Parents seek to hold Snap liable for its role in violating its distinct duty to design a reasonably safe product.”

The “no treatment as a publisher” claims have not always succeeded. For instance, in 2017, Matthew Herrick sued Grindr after his ex-boyfriend used the dating app to impersonate Herrick and post profiles stating that he was interested in “serious kink and many fantasy scenes,” causing more than 1,000 people to respond, with many arriving at his home and work due to Grindr’s geolocation function.¹⁴⁹ Despite receiving more than 100 complaints from Herrick and others about these fake accounts, Grindr did nothing other than

144. *Id.* at 851.

145. *Id.*

146. *Lemmon v. Snap*, 995 F.3d 1085 (9th Cir. 2021).

147. *Id.*

148. *Id.*

149. *Herrick v. Grindr, LLC*, 306 F. Supp. 3d 579, 585 (S.D.N.Y. 2018).

send an automated reply, Herrick's complaint alleged.¹⁵⁰ Herrick's lawsuit against Grindr focused on the dangerous nature of the app and the failure to incorporate basic safety features. The lawsuit included claims for negligence, deceptive business practices and false advertising, emotional distress, failure to warn, negligent misrepresentation, products liability, negligent design, promissory estoppel, and fraud.¹⁵¹

Relying on the Ninth Circuit's *Internet Brands* opinion, Herrick argued that § 230 did not apply to his failure to warn claim, but the district court rejected the comparison. "By contrast, the proposed warning in this case would be about user-generated content itself—the impersonating profiles or the risk that Grindr could be used to post impersonating or false profiles," the district court wrote.¹⁵² "Unlike in *Internet Brands*, Herrick's failure-to-warn claim depends on a close connection between the proposed warning and user-generated content."¹⁵³ The district court concluded that the other claims were either also immunized under § 230 or inadequately pled.¹⁵⁴ The Second Circuit affirmed the district court's dismissal in a nonprecedential summary order,¹⁵⁵ and the U.S. Supreme Court denied certiorari.¹⁵⁶

C. JUDICIAL CALLS FOR § 230 REFORM

Despite the abrogation of § 230 at the edges, Judge Wilkinson's primary holding in *Zeran*—that the prohibition on treating interactive computer service providers as publishers includes a ban on distributor liability—has gone largely unchallenged by judges over the past quarter century. The Supreme Court has never interpreted the scope of § 230, but Justice Thomas appears eager not only to take a § 230 case, but to challenge the broad *Zeran* reading of the statute. In a 2020 statement accompanying the Supreme Court's denial of certiorari in a case involving § 230(c)(2), Justice Thomas wrote that "there are good reasons to question" the broad *Zeran* reading that extends § 230(c)(1) to distributor liability.¹⁵⁷ He also criticized courts' broad application of § 230. "Paring back the sweeping immunity courts have read into § 230 would not necessarily render defendants liable for online misconduct," Thomas wrote.

150. *Id.*

151. *Id.* at 586-87.

152. *Id.* at 592.

153. *Id.*

154. *Id.* at 601.

155. *Herrick v. Grindr, LLC*, No. 18-396 (2d Cir. Mar. 27, 2019).

156. *Herrick v. Grindr, LLC*, 140 S. Ct. 221 (2019).

157. *Malwarebytes v. Enigma Software Grp.*, 141 S. Ct. *13, *18 (2020) (Thomas, J., concurring in denial of certiorari).

“It simply would give plaintiffs a chance to raise their claims in the first place.”¹⁵⁸

It is unclear whether other Supreme Court Justices share Justice Thomas’s views on § 230. The Court’s denial of certiorari in *Herrick* and other § 230 cases suggests that the Supreme Court is not eager to wade into the statute any time soon.

In recent years, some federal appellate court judges have written individual concurrences and dissents in which they express frustration with the breadth of § 230’s protections. Perhaps the most notable example was a 2016 opinion affirming the § 230-based dismissal of sex trafficking-related claims against Backpage. The First Circuit concluded the opinion by noting the plaintiff’s argument that Backpage enabled sex trafficking. “But Congress did not sound an uncertain trumpet when it enacted the CDA, and it chose to grant broad protections to internet publishers,” Judge Selya wrote for the unanimous three-judge panel, which included retired Supreme Court Justice Souter. “Showing that a website operates through a meretricious business model is not enough to strip away those protections. If the evils that the appellants have identified are deemed to outweigh the First Amendment values that drive the CDA, the remedy is through legislation, not through litigation.”¹⁵⁹

Congress responded within two years, passing the first ever substantive amendment to § 230, abrogating the immunity for some civil actions and state criminal prosecutions involving sex trafficking.¹⁶⁰ Congress has not amended § 230 since 2018, but other judges have called on legislators to consider changes to the statute.

Consider the late Judge Katzmann’s separate partial concurrence in a Second Circuit opinion that affirmed the § 230 dismissal of claims against Facebook that arose from its alleged violation of the Anti-Terrorism Act by provisioning a platform to Hamas and using “sophisticated algorithms” to present Hamas content to users.¹⁶¹

Section 230, Judge Katzmann wrote, does not necessarily apply to claims surrounding Facebook’s promotion of content.

“First, Facebook uses the algorithms to create and communicate its own message: that it thinks you, the reader—you, specifically—will like this

158. *Id.*

159. *Doe v. Backpage*, 817 F.3d 12 (1st Cir. 2016).

160. Allow States and Victims to Fight Online Sex Trafficking Act (“FOSTA”), Pub. L. No. 115-164, 132 Stat. 1253 (2018).

161. *Force v. Facebook, Inc.*, 934 F.3d 53, 77 (2d Cir. 2019) (Katzmann, J., partial concurrence and partial dissent).

content,” he wrote. “And second, Facebook’s suggestions contribute to the creation of real-world social networks. The result of at least some suggestions is not just that the user consumes a third party’s content.”¹⁶²

Although § 230 protects Facebook for the publication of third-party content, Judge Katzmman reasoned, the statute does not protect it for claims arising from Facebook’s use of that content. This is in line with the approach of circumventing § 230 by arguing that the claims do not treat the platform as the publisher or speaker of third-party content. According to Katzmman, “it strains the English language to say that in targeting and recommending these writings to users—and thereby forging connections, developing new social networks—Facebook is acting as ‘the *publisher* of information provided by another information content provider.”¹⁶³

Judge Katzmman concluded his opinion with a call for Congress to consider whether § 230 continues to serve the purposes for which it was passed in 1996. “The text and legislative history of the statute shout to the rafters Congress’s focus on reducing children’s access to adult material,” he wrote. “Congress could not have anticipated the pernicious spread of hate and violence that the rise of social media likely has since fomented. Nor could Congress have divined the role that social media providers themselves would play in this tale.”¹⁶⁴

Judge Katzmman has not been the only judge to write a separate opinion urging a more modest interpretation of § 230. In a partial concurrence and partial dissent in a similar Anti-Terrorism Act case in 2021, Judge Gould of the Ninth Circuit also argued that § 230 does not apply to platforms’ use of algorithms.¹⁶⁵

Largely echoing Katzmman’s partial dissent, in *Gonzalez v. Google*, Gould wrote that he would prefer for Congress and the executive branch to “seriously grapple” with the many social problems that arise from a lack of regulation of social media:

But if Congress continues to sleep at the switch of social media regulation in the face of courts broadening what appears to have been its initial and literal language and expressed intention under § 230, then it must fall to the federal courts to consider

162. *Id.* at 82

163. *Id.* at 76-77 (emphasis added) (quoting 47 U.S.C. § 230(c)(1)).

164. *Id.* at 88.

165. *Gonzalez v. Google, LLC*, 2 F.4th 871 (9th Cir. 2021), *reh’g en banc denied*, 21 F.4th 665 (9th Cir. 2022) (Gould, J., concurring).

rectifying those errors itself by providing remedies to those who are injured by dangerous and unreasonable conduct.¹⁶⁶

Gould linked the lack of social media regulation to current political problems such as election misinformation, writing about concerns that social media platforms can “distort and tribalize public opinion, to spread falsehoods as well as truth, and to funnel like-minded news reports to groups in a way that makes them think there are ‘alternative facts’ or ‘competing realities’ that exist, rather than recognize more correctly that there are ‘truth’ and ‘lies.’”¹⁶⁷ In October 2022, the Supreme Court granted certiorari in *Gonzales*, marking the first time that the Court has agreed to interpret Section 230.

Even if the Supreme Court retains the broad *Zeran* precedent, Congress might narrow it. The separate opinions of Judge Gould and Judge Katzmann are not binding precedent, but they are remarkable in that federal judges are writing not only to state their interpretations of the law but to urge Congress to consider changing § 230. It remains to be seen whether their opinions will have the same impact as Judge Selya’s and cause Congress to further amend the law. But since 2019, members of Congress have introduced more than thirty-five bills that would either amend or repeal § 230.¹⁶⁸ Some bills aim to reduce the discretion that platforms have in blocking content and suspending users, such as by imposing viewpoint neutrality requirements on moderation.¹⁶⁹ Other bills impose a duty of care on platforms to encourage them to block harmful content more aggressively.¹⁷⁰ And some bills exempt from § 230’s protections particular types of harmful third-party content, such as civil rights violations and harassment.¹⁷¹

IV. PRINCIPLES FOR § 230 REFORM

Analyzing each of the proposed § 230 reform bills would be of limited use for a law review article, as the list of proposals likely will continue to grow and, as of the time of publication, no bill appears to be particularly likely to pass. Some bills carve out particular categories of claims from § 230 protection, others impose new procedural requirements on platforms, some restrict the

166. *Id.*

167. *Id.*

168. Meghan Anand, Kiran Jeevanjee, Daniel Johnson, Brian Lim, Irene Ly, Matt Perault, Jenna Ruddock, Tim Schmeling, Niharika Vatikonda, Noelle Wilson & Joyce Zhou, *All the Ways Congress Wants to Change Section 230*, SLATE (Feb. 11, 2022, 5:45 AM), <https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html>.

169. *Id.*

170. *Id.*

171. *Id.*

ability of platforms to moderate content, and others repeal the law entirely.¹⁷² Indeed, with some bills aiming to reduce the amount of moderation that platforms perform and others seeking to increase the amount of moderation, it is hard to conceive of an easy consensus that addresses all concerns.

This Part will instead briefly suggest principles that Congress should keep in mind as it considers these proposals and develops new ones—or decides to refrain from § 230 changes. I do not suggest that Congress should carve § 230 into stone for eternity; it is a statute that Congress can and should assess regularly. But as this Part argues, § 230 changes cannot address every problem with the internet. Moreover, changes to the statute may have unintended consequences.

A. ELIMINATING § 230 WON'T ELIMINATE THE FIRST AMENDMENT

As the subsequently corrected *New York Times* headline about hate speech shows, commentators often blame § 230 for harmful speech that the First Amendment protects, no matter if § 230 is on the books. If Congress were to repeal § 230 tomorrow, it still could not constitutionally pass a law that holds platforms liable for online hate speech.¹⁷³ Nor could Congress pass a statute that imposes a blanket prohibition on platforms' distribution of disinformation, as the First Amendment protects many types of lies.¹⁷⁴

The First Amendment not only prohibits the government from directly banning protected speech; it also prohibits the government from requiring platforms to ban that speech. As a corollary, the First Amendment does not prohibit platforms from independently deciding to block that same speech. This is due to the state action doctrine, the principle that the First Amendment generally only restricts the actions of the government and not the voluntary actions of private parties that do not involve government intervention.¹⁷⁵ As

172. For a good summary of the pending § 230 bills, see *id.* For an analysis of the different types of proposals, see Mark A. Lemley, *The Contradictions of Platform Regulation*, 1 J. FREE SPEECH L. 303 (2021).

173. See *Matal v. Tam*, 137 S. Ct. 1744, 1764 (2017) (“Speech that demeans on the basis of race, ethnicity, gender, religion, age, disability, or any other similar ground is hateful; but the proudest boast of our free speech jurisprudence is that we protect the freedom to express the thought that we hate.”) (internal quotation marks and citation omitted).

174. See *United States v. Alvarez*, 567 U.S. 709, 732 (2012) (plurality) (“The remedy for speech that is false is speech that is true. This is the ordinary course in a free society. The response to the unreasoned is the rational; to the uninformed, the enlightened; to the straightout lie, the simple truth.”).

175. See *Manhattan Comty. Access Corp. v. Halleck*, 139 S. Ct. 1921, 1925 (2019) (“The Free Speech Clause of the First Amendment constrains governmental actors and protects

Justice Kavanaugh wrote in 2019, only in “a few limited circumstances” can a private company be a state actor for First Amendment purposes: “(i) when the private entity performs a traditional, exclusive public function; (ii) when the government compels the private entity to take a particular action; or (iii) when the government acts jointly with the private entity.”¹⁷⁶

Kavanaugh’s second exception could raise issues for government-imposed moderation mandates for platforms because a court likely would view any legal requirement to moderate as government compulsion. And the third exception makes it difficult for platforms to voluntarily partner with the government to identify and block harmful user content and actors, as such a partnership could be seen as a joint action with the government.

But when platforms independently and voluntarily adopt content moderation policies and procedures, the First Amendment does not constrain their decisions.¹⁷⁷ This freedom from the First Amendment’s constraints has enabled platforms to ban constitutionally protected content such as hate speech and misinformation.

Section 230 helps provide the platforms with this flexibility. Section 230(c)(2) explicitly provides immunity for good-faith efforts to block objectionable content, but the First Amendment also protects such editorial discretion.¹⁷⁸ Section 230(c)(1) has perhaps been even more important than § 230(c)(2) in providing platforms with the breathing space to moderate constitutionally protected content. Although the First Amendment protects the platforms’ ability to moderate this content, § 230(c)(1) has precluded more courts from adopting the *Stratton Oakmont* rule and holding platforms liable for all user content that they leave up just because they have moderated some content. To be sure, there is a strong argument that *Stratton Oakmont*

private actors. To draw the line between governmental and private, this Court applies what is known as the state-action doctrine.”).

176. *Id.* at 1928 (cleaned up).

177. *See* *Prager Univ. v. Google, LLC*, 951 F.3d 991, 994 (9th Cir. 2020) (“Despite YouTube’s ubiquity and its role as a public-facing platform, it remains a private forum, not a public forum subject to judicial scrutiny under the First Amendment.”); *Howard v. America Online*, 208 F.3d 741, 754 (9th Cir. 2000) (“There is nothing in the record that supports the contention that AOL should be considered a state actor.”).

178. *See* *Miami Herald Publ’g v. Tornillo*, 418 U.S. 241, 258 (1974) (“The choice of material to go into a newspaper, and the decisions made as to limitations on the size and content of the paper, and treatment of public issues and public officials—whether fair or unfair—constitute the exercise of editorial control and judgment. It has yet to be demonstrated how governmental regulation of this crucial process can be exercised consistent with First Amendment guarantees of a free press as they have evolved to this time.”).

misinterpreted the common law of distributor liability,¹⁷⁹ but few other cases interpret this area of the law as applied to the internet.

If Congress amends § 230, it should ensure that it does not recreate the perverse incentive of *Stratton Oakmont*. Eliminating § 230(c)(1) entirely runs the risk of such an outcome. A slightly narrower amendment, dictating that online services are the distributors but not the publishers of third-party content, could help to avoid a *Stratton Oakmont* outcome. Yet as the next Section argues, even this semi-repeal of § 230(c)(1) could have substantial unintended consequences.

B. § 230 PROVIDES CERTAINTY TO PLATFORMS

Imagine if Congress did, in fact, amend § 230 to impose distributor liability on all online platforms.¹⁸⁰ Or, absent an amendment, the Supreme Court could follow Justice Thomas's lead and reject *Zeran*, leading to the same outcome.

We cannot say precisely what a distributor liability regime would look like for online platforms. Section 230's existence since the dawn of the modern internet has obviated the need for courts to apply common law distributor liability standards to online platforms. If platforms were considered distributors, they would face liability if they (1) knew or (2) had reason to know of defamatory or otherwise unlawful user content.

What does it mean for a platform to “know” about defamatory or unlawful user content? At the very least, the platform could face liability if it had actual knowledge of the content. Under *Hamling*, liability would not hinge on the platform's knowledge that the content was illegal; merely knowing about the particular content would suffice.¹⁸¹ Such a standard could create a notice-and-takedown regime under which an aggrieved party could establish the platform's “knowledge” by notifying the platform. For instance, consider a restaurant that is unhappy with a Yelp review claiming that the chicken it served was partly raw. If the restaurant complained to Yelp that the review was inaccurate, the restaurant could then argue that Yelp had knowledge of the allegedly defamatory review. Yelp would then face the prospect of defending a defamation suit on the merits in court. Yelp likely cannot afford to investigate whether the restaurant actually served raw chicken, so its most prudent response would be to remove the review.

179. See Mike Godwin, CYBER RIGHTS: DEFENDING FREE SPEECH IN THE DIGITAL AGE 97 (2003) (“Logically, Justice Ain's interpretation of *Cubby v. CompuServe* makes no sense.”).

180. See H.R. 2000, 117th Cong. (2021) (stating that Section 230 shall not “be construed to prevent a provider or user of an interactive computer service from being treated as the distributor of information provided by another information content provider”).

181. See *supra* Section II.A.

But under the common law, distributors also face liability if they had “reason to know” of the defamatory or unlawful content. The courts have not explained when a distributor has a “reason to know” of user content but, by its very terms, it encompasses a broader range of scenarios than actual knowledge. Shortly after § 230 was passed in 1996—when it appeared that the statute merely overruled *Stratton Oakmont*—Floyd Abrams wrote an article that warned of the uncertainty created by imposing liability if an online service had ‘reason to know’ of the user content.

“Is this a negligence standard underprotective of on-line providers and their First Amendment rights?” Abrams wrote. “It sure sounds a lot less protective than *New York Times v. Sullivan*, which is the opposite of ‘reason to know’ and applies a standard of actual knowledge or actual serious doubts as to truth or falsity.”¹⁸²

Because the Fourth Circuit issued *Zeran* the next year, Abrams’s concerns about distributor liability for online platforms remained hypothetical. *Zeran*—and its widespread adoption by courts nationwide—meant that whether a platform knew or had reason to know of particular user content was irrelevant for liability purposes.

A repeal of or substantial amendment to § 230 could bring back the uncertainty that Abrams highlighted in 1996. Social media providers, consumer review sites, community bulletin boards, and other platforms would scramble to determine when they know or have reason to know of user content. Smaller platforms with limited legal resources might decide to eliminate venues for user-generated content.

Unless courts provide sufficient certainty about the protections that platforms receive under a distributor liability regime, a rational platform would err on the side of taking down user content that might be defamatory or otherwise lead to potential liability. At the very least, distributor liability would create a notice-and-takedown system, allowing aggrieved individuals to pressure platforms to take down user content. But platforms might be even more risk averse due to the vague “reason to know” standard and proactively remove controversial content even without receiving a complaint.

To some critics of § 230—particularly those who believe that platforms do not adequately moderate harmful content—this very well may be a welcome change. Under a distributor liability system, platforms would have a substantial incentive to block harmful content. The downside is that they also would block content that is not necessarily harmful or illegal; overfiltering is a given when

182. Floyd Abrams, *First Amendment Postcards from the Edge of Cyberspace*, 11 ST. JOHN’S J. LEGAL COMMENT 693, 704 (1996).

moderating content at scale (and, as described in Section IV.D of this Article, there often is not a “correct” decision about moderation). The § 230 critics who believe that platforms already block too much user content would be particularly disappointed by a distributor liability system as risk-averse platforms would block more content than they otherwise would with the full § 230 protections in place. Indeed, the notice-and-takedown regime for copyright claims under § 512 of the Digital Millennium Copyright Act has resulted in platforms often being risk averse and taking down disputed user content to avoid liability.¹⁸³

C. § 230 CARVEOUTS CAN HAVE SWEEPING IMPACTS

Not all § 230 reform proposals would entirely remove the statute’s broad protections for platforms. Some proposals would retain the core protections of § 230(c)(1) but exempt particular types of claims. For instance, the Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act, introduced in the Senate in February 2021, would remove § 230 protections for claims involving civil rights, antitrust, stalking, harassment, intimidation, international human rights law, and wrongful death.¹⁸⁴ The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act, introduced in 2020, would remove § 230 protections for certain civil claims and state criminal prosecutions involving child sex abuse material.¹⁸⁵

Carve-outs to § 230 are an attractive alternative to complete overhauls or repeals of liability protection. The categories of content described above are harmful and often deplorable. The challenge, however, is to avoid incentives for platforms to overcensor content that does not fall within those categories.

Like all businesses, platforms have lawyers. And lawyers are understandably risk averse, particularly when the liability rules are unclear. If Congress changes the law to impose more potential liability for particular types of content, platforms likely will more aggressively moderate not only the content that is clearly illegal but other user content that could possibly fall within that category. Even if it is unclear whether the § 230 exception would

183. See Corynne McSherry, *Platform Censorship: Lessons from the Copyright Wars* ELECTRONIC FRONTIER FOUNDATION (Sept. 26, 2018), <https://www EFF.ORG/deeplinks/2018/09/platform-censorship-lessons-copyright-wars> (“Many takedowns target clearly infringing content. But there is ample evidence that rightsholders and others abuse this power on a regular basis—either deliberately or because they have not bothered to learn enough about copyright law to determine whether the content to which they object is actually unlawful.”).

184. S. 299, 117th Cong. § 2 (2021).

185. S. 3398.

apply, or whether the platform would face liability without § 230 protection, the platform would likely avoid risking the cost of litigating a case on the merits.

The only significant amendment to § 230 provides a case study as to how platforms react to new § 230 exceptions. The 2018 sex trafficking law, the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA),¹⁸⁶ created new exceptions to § 230 for civil claims under a federal sex trafficking law and state criminal prosecutions would constitute violations of certain federal criminal laws regarding sex trafficking and the promotion or facilitation of prostitution.¹⁸⁷

Within days of FOSTA's passage, online classified ad site Craigslist removed its entire personal ad section. "Any tool or service can be misused," the site wrote. "We can't take such risk without jeopardizing all our other services, so we have regretfully taken craigslist personals offline. Hopefully we can bring them back some day."¹⁸⁸ Personals ads serve a wide range of lawful purposes. But because they potentially could be misused by sex traffickers—and the scope of liability under FOSTA was unknown—Craigslist made the risk-based decision to remove the entire personals ads section.

FOSTA's enactment—along with the FBI's seizure of Backpage a few days before FOSTA was signed into law¹⁸⁹—reduced the availability of platforms for sex workers. The lack of online platforms has reportedly driven many sex workers to bars or streets, increasing the danger that they face.¹⁹⁰ After conducting an online survey of ninety-eight sex workers, Danielle Blunt and Ariel Wolf concluded that FOSTA "has created an environment where marginalised populations are pushed into increased financial insecurity, which, in turn, makes them more vulnerable to labour exploitation and trafficking in the sex industry."¹⁹¹ A 2021 *Columbia Human Rights Law Review* article summarized the impacts of FOSTA:

186. Allow States and Victims to Fight Online Sex Trafficking Act ("FOSTA"), Pub. L. No. 115-164, 132 Stat. 1253 (2018).

187. *Id.*

188. FOSTA, CRAIGSLIST, <https://www.craigslist.org/about/FOSTA> (last visited May 16, 2022).

189. Daniel Oberhaus, *The FBI Just Seized Backpage.com*, VICE (Apr. 6, 2018).

190. See Dean DeChiaro, *Sex Workers, Sidelined in Last Section 230 Debate, Seek a Seat at the Table*, ROLL CALL (Feb. 23, 2021), <https://rollcall.com/2021/02/23/sex-workers-sidelined-in-last-section-230-debate-seek-a-seat-at-the-table/>.

191. Danielle Blunt & Ariel Wolf, *Erased: The Impact of FOSTA-SESTA and the Removal of Backpage on Sex Workers*, 14 ANTI-TRAFFICKING R. 117 (2020).

The result is that people in the sex trades, who work in legal, semi-legal, and criminalized industries, have been forced into dangerous and potentially life-threatening scenarios. Many no longer have access to affordable methods of advertising and have returned to outdoor work or to in-person client-seeking in bars and clubs, where screening of the type that occurs online is impossible, and where workers are more vulnerable to both clients and law enforcement. These effects have been most impactful on sex workers facing multiple forms of marginalization, including Black, brown, and Indigenous workers, trans workers, and workers from lower socio-economic classes, who are prohibited from or unable to access more expensive advertising sites that may not be as impacted by FOSTA.¹⁹²

FOSTA was a well-intentioned amendment to § 230 that sought to address the very real problem of sex trafficking. It is unclear whether FOSTA actually reduced sex trafficking, as other means are available to sex traffickers besides public-facing websites that are most likely to care about § 230. But we do know that FOSTA's impacts reached far beyond sex trafficking and that platforms' reactions to the increased liability has made life more dangerous for sex workers.

The fallout from FOSTA suggests that platforms will react quickly and in a risk-averse manner to new § 230 exceptions. Given the uncertainty created by the new potential liability, many platforms likely will block content that might even possibly fall within the exception. Accordingly, Congress should create new § 230 carveouts with great care, conscious of the unintended consequences of the new liability.

D. "NEUTRALITY" IS ELUSIVE

Other § 230 proposals seek to limit platforms' ability to moderate user content. These bills often stem from concerns that platforms are politically biased and unequally censor certain political views (often those of conservatives). For instance, the Protecting Constitutional Rights from Online Platform Censorship Act, introduced in the House in January 2021, would prohibit platforms from taking "any action to restrict access to or the availability of" First Amendment-protected user content."¹⁹³ The Stop Suppressing Speech Act, introduced in October 2020, would amend

192. Kendra Albert, Elizabeth Brundige & Lorelei Lee, *FOSTA in Legal Context*, 52 COLUM. HUM. RTS. L. REV. 1084, 1089-90 (2021).

193. H.R. 83, 117th Cong. (2021).

§ 230(c)(2) so that it only applies to a narrower category of user content, including that which promotes violence or terrorism.¹⁹⁴

The proposals often stem from a common misrepresentation that § 230 only applies to “neutral platforms.”¹⁹⁵ As explained in Part I.B, Congress passed § 230 to overturn the perverse incentives created by *Stratton Oakmont* and provide platforms with the flexibility to moderate user content without suddenly becoming liable for everything on their sites.¹⁹⁶ Some critics who acknowledge that § 230 does not require neutrality argue that it should do so, and they suggest amending the law to impose a neutrality or common carriage requirement.¹⁹⁷

From their perspective, § 230 provides online platforms with protection that goes beyond that of the First Amendment—protection that offline media do not enjoy. If platforms receive § 230 protection, they argue, the platforms should not moderate in a biased manner. Although the desire for “neutral platforms” might be understandable, on closer review it is impossible to achieve (and even if it were possible, it would not be desirable).

To see why, begin with a simple question: What does it mean for a platform to be neutral? Does it mean that the platform should not engage in any moderation at all? Such a policy could result in a torrent of harmful and illegal content. For instance, in the first quarter of 2021, Facebook took action on five million pieces of content that violated its child nudity and sexual exploitation policies.¹⁹⁸ Few people would argue that such content should remain on a public platform.

194. S. 4828, 116th Cong. (2020).

195. See Catherine Padhi, *Ted Cruz vs. Section 230: Misrepresenting the Communications Decency Act*, LAWFARE (Apr. 20, 2018), <https://www.lawfareblog.com/ted-cruz-vs-section-230-misrepresenting-communications-decency-act> (quoting Sen. Ted Cruz as saying to Facebook CEO Mark Zuckerberg, “The predicate for Section 230 immunity under the CDA is that you’re a neutral public forum. Do you consider yourself a neutral public forum, or are you engaged in political speech, which is your right under the First Amendment.”).

196. See Adi Robertson, *Why the Internet’s Most Important Law Exists and How People Are Still Getting It Wrong*, THE VERGE (June 21, 2019) (“They wanted platforms to feel free to make these judgments without risking the liability that Prodigy faced.”).

197. See, e.g., Adam Candeub, *Bargaining for Free Speech: Common Carriage, Network Neutrality, and Section 230*, 22 YALE J.L. TECH. 391, 433 (2020) (“These reforms would include an antidiscrimination requirement or requirements that dominant platforms share blocking technologies with users so that individuals, not corporate platforms, set the boundaries of on-line speech.”).

198. See *Community Standards Enforcement Report*, META (2021), <https://transparency.fb.com/data/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/>.

A slightly more refined version of the neutrality argument is that platforms should only receive § 230 protections if they allow all constitutionally protected content on their services. Because child sex abuse material is categorically not constitutionally protected such a requirement would still permit a platform to block that content. But platforms also moderate a great deal of content that many would agree should be blocked. Would content that qualifies as commercial speech for First Amendment analysis be covered by a neutrality requirement? For instance, Facebook in the first quarter of 2021 took action on 905 million pieces of content that violated its spam policies.¹⁹⁹ Few would argue that the internet would benefit from more spam.

Another version of the neutrality argument is that platforms should be permitted to moderate content—even content that is constitutionally protected—provided that the platforms engage moderate in a “viewpoint neutral” manner. Although that sounds slightly more reasonable, it also is difficult to conceive of how such a policy would work in practice. For instance, in the first quarter of 2021, Facebook took action on about 25 million pieces of content under its hate speech policy.²⁰⁰ Facebook’s detailed hate speech policy contains a long list of the types of attacks on individuals prohibited on the platform.²⁰¹ Online political arguments can get heated, and often include hateful remarks. The decision to include or exclude a particular type of speech within the definition of hate speech might be seen as politically biased. Depending on how it is drafted, a viewpoint neutrality requirement might preclude a platform from banning hate speech and other constitutionally protected content.

Content moderation is difficult, particularly when dealing with up to thousands of pieces of user content a second. Setting policies and identifying content that violates those policies is a tall task, and it is impossible to satisfy everyone, in part because users have different expectations and understandings of what kind of content is harmful. Consider the coronavirus pandemic. In 2020, the theory that COVID-19 originated from a lab in China was largely criticized. But in 2021, more mainstream commentators and politicians began to find the theory at least plausible. Should a social media site have classified the lab leak theory as misinformation in 2020 and taken down any posts containing it? What about in 2021? Or should the platforms have been *required* to carry the theory in 2021, under the assumption that the platforms must be “neutral?” What about in 2020? All of these questions are hard, and the system

199. *Id.*

200. *Id.*

201. *Hate Speech*, META <https://transparency.fb.com/de-de/policies/community-standards/hate-speech/> (last visited May 18, 2022).

under § 230 and the First Amendment provides platforms with the flexibility to make these decisions.

Indeed, § 230 is very much a free market-based law that assumes that by providing platforms with the breathing room to set their own policies, they will best meet the demands of many of their users. If platforms are too restrictive or not restrictive enough, at least according to the theory, users will migrate to another platform. Of course, this market-based theory may not function smoothly if there is not sufficient competition for the largest platforms. But imposing a neutrality requirement would not necessarily solve this problem, as it would overwhelm platforms with content that makes the overall user experience less pleasant, and in some cases, more dangerous.

In short, “neutral platforms” is a tempting proposition. But a world in which platforms were entirely neutral would have sweeping negative consequences for the internet, causing it to be filled with spam, illegal images, violence, and so many other things that most users would expect platforms to block. A modified version of neutrality might avoid some of the worst outcomes, but it is difficult to imagine consensus on a more flexible view of “neutrality.”

E. TRANSPARENCY COULD IMPROVE THE § 230 DEBATE

Much of the § 230 debate has been driven by widespread misunderstandings—innocent or otherwise. Some of these misunderstandings involve easily corrected legal errors. No, § 230 does not require neutrality.²⁰² No, repealing § 230 would not suddenly create a cause of action for

202. Catherine Padhi, *Ted Cruz vs. Section 230: Misrepresenting the Communications Decency Act*, LAWFARE (Apr. 20, 2018, 10:00 AM), <https://www.lawfareblog.com/ted-cruz-vs-section-230-misrepresenting-communications-decency-act> (“Sen. Ted Cruz, the Republican from Texas, suggested as much while questioning Facebook CEO Mark Zuckerberg during last week’s congressional hearings. But Cruz’s representation of Section 230 is misleading. There is no requirement that a platform remain neutral in order to maintain Section 230 immunity. And Facebook does not have to choose between the protections of Section 230 and those of the First Amendment; it can have both.”).

constitutionally protected speech.²⁰³ No, § 230 does not apply to copyright infringement claims.²⁰⁴

But other misunderstandings come from the complex nature of moderating content at scale. Under § 230's protections, platforms have voluntarily developed detailed policies and procedures for constitutionally protected but objectionable user content. The policies are not merely choices of whether to take down or leave up content; they have a long menu of options that they believe are in the best interests of their users (and their businesses). Eric Goldman has documented the wide range of remedies beyond takedowns. They include relocating content, suspending accounts, using credibility badges, demonetizing content, educating users, and reducing service levels.²⁰⁵

Goldman's work is part of a growing body of scholarship that has begun to provide some transparency as to how platforms moderate content at scale. Sarah Roberts has documented the lives of the workers who moderate the content for social media companies.²⁰⁶ Kate Klonick has traced the history of the earliest social media content moderation policies²⁰⁷ and the development of the Facebook Oversight Board.²⁰⁸ And evelyn douek has explained the role of international human rights law in content moderation.²⁰⁹ More than a decade ago, Danielle Citron highlighted the persistent harassment that people face online and proposed solutions.²¹⁰ These works demonstrate the nuances and complexities of content moderation. Unfortunately, this scholarship has

203. Betsy Klein, White House reviewing Section 230 amid efforts to push social media giants to crack down on misinformation, CNN (July 20, 2021) ("The Section 230 debate is taking on new urgency in recent days as the administration has called on social media platforms to take a more aggressive stance on combating misinformation. The federal law, which is part of the Communications Decency Act, provides legal immunity to websites that moderate user-generated content.").

204. See Andrew Marantz, *Free Speech is Killing Us*, N.Y. Times (Oct. 4, 2019) <https://www.nytimes.com/2019/10/04/opinion/sunday/free-speech-social-media-violence.html> (correcting opinion piece to state that "[a]n earlier version of this article misidentified the law containing a provision providing safe haven to social media platforms. It is the Communications Decency Act, not the Digital Millennium Copyright Act.").

205. Eric Goldman, *Content Moderation Remedies*, 28 MICH. TECH. L. R. 1 (2021).

206. Sarah Roberts, BEHIND THE SCREEN: CONTENT MODERATION IN THE SHADOWS OF SOCIAL MEDIA (2019).

207. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018).

208. Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 YALE L. J. 2232 (2020).

209. evelyn douek, *The Limits of International Law in Content Moderation*, 6 UCI J. OF INT'L, TRANSNATIONAL, AND COMP. L. 37 (2021).

210. Danielle Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009).

not fully informed the debate in the popular media and Congress, where misconceptions continue to proliferate.

To address this knowledge gap, Congress should consider forming a nonpartisan commission of experts to gather facts about how content moderation currently works, what is possible, and how changes in the law might positively or negatively affect the field. As I wrote in a 2019 proposal for such a commission, other congressional commissions in areas such as national security and cybersecurity have helped to develop informed records and thoughtful proposals.²¹¹ As one example, the 2020 defense authorization bill contained twenty-five recommendations from the Cyberspace Solarium Commission, which Congress had formed to gather facts and shape policy about emerging cyber threats.²¹²

A nonpartisan content moderation commission would be an alternative to the current discourse around § 230, which has seen dozens of conflicting proposals but very few facts about how content moderation actually works and how these bills would change the system. As seen with FOSTA, even a change to one narrow area of user content can have substantial effects on platforms' behavior.

Transparency also can come from the platforms. Many large and small platforms publicly post user content policies with varying degrees of detail. Some platforms, such as Facebook and Google, also publish transparency reports that at least provide some statistics about the content that they have removed. This is a good first step, and Congress should consider ways to better foster this transparency. For instance, the Platform Accountability and Consumer Transparency Act,²¹³ introduced in 2020 and 2021, would, among other things, require platforms to publish content moderation statistics and accessible content moderation policies. Platforms still would have the flexibility to establish moderation practices that they believe their users demand, but a transparency requirement would better inform their users and help § 230's market-based system function more efficiently. Even these more modest proposals would need close examination for First Amendment concerns. For instance, could a law require a newspaper to disclose how and

211. Jeff Kosseff, *Understand the Internet's Most Important Law Before Changing It*, REG. REV. (Oct. 10, 2019).

212. See Press Release, Cyberspace Solarium Commission, *NDAA Enacts 25 Recommendations from the Bipartisan Cyberspace Solarium Commission* (Jan. 2, 2021).

213. Platform Accountability and Consumer Transparency Act, S. 4066, 116th Cong. (2020).

why it decides which letters to publish or how it edits stories?²¹⁴ If not, conditioning § 230 protections on such transparency also could raise constitutional concerns.²¹⁵

V. CONCLUSION

This Article has sought to provide some clarity to the increasingly heated debate surrounding § 230. Understanding § 230's history, purpose, and mechanics is crucial in debating its future. This Article has a cautionary tone and explains how even minor changes to § 230 could have substantial (and perhaps unintended) consequences on content moderation and the everyday internet experience. The intention is not to suggest that Congress should avoid making any changes to § 230. No law is perfect, and the internet that Section 230 has shaped also is far from ideal. But our dissatisfaction with the current state of the internet is not a valid excuse for making sweeping changes to a fundamental internet law without fully considering the impacts that those changes would have. This Article has sought to inform what hopefully will be a more substantive and reality-based debate about the future of § 230 and online platforms.

214. See Eric Goldman, *Comments on the Platform Accountability and Consumer Transparency Act (the "PACT Act")* (July 27, 2020), <https://blog.ericgoldman.org/archives/2020/07/comments-on-the-platform-accountability-and-consumer-transparency-act-the-pact-act.htm>.

215. See *Elrod v. Burns*, 427 U.S. 347, 361 (1976) ("The denial of a public benefit may not be used by the government for the purpose of creating an incentive enabling it to achieve what it may not command directly.").

THE DYSTOPIAN RIGHT OF PUBLICITY

Dustin Marlan[†]

ABSTRACT

Our society frequently describes privacy problems with the dystopian metaphor of George Orwell's *1984*. Understood through the Orwellian metaphor—and particularly the “Big Brother is watching you” maxim—privacy rights are forcefully invaded by the government's constant surveillance and disclosures of personal information. Yet our other personality right—the right of publicity, “the right of every human being to control the commercial use of his or her identity”—still lacks an appropriate metaphor, making it difficult to conceptualize and thus to regulate effectively.

This Article suggests that the problems with a commercially transferable right of publicity can be usefully analogized to another chilling dystopia: Aldous Huxley's *Brave New World*. Huxley wrote *Brave New World* as an expression of the anxiety of losing one's individual identity in a technology-driven future. The novel envisioned a utilitarian society controlled through technological manipulation, conspicuous consumption, social conditioning, and entertainment addiction. In contrast to Orwell's Big Brother's forceful coercion, pacified citizens in Huxley's “World State” society willingly participate in their own servitude.

Commentators often focus on the fact that litigated publicity cases tend to overprotect celebrities' fame to the detriment of creators' First Amendment rights. The vast majority of publicity rights, however, actually belong to ordinary citizens. The Huxleyan metaphor's depiction of technological manipulation, social conditioning, and identity loss thus reveals the constant but overlooked publicity problem that this Article labels the “pleasurable servitude.” In effect, by consenting to terms of service on social media, ordinary citizens voluntarily license rights in their identities to internet platforms in exchange for access to the pleasures of digital realities. Through this unregulated mass transfer of publicity rights, social networks strip away their users' identities and sell them to advertisers as commodities. This Article claims that pleasurable servitude is a form of surveillance capitalism deserving of regulation by means of “publicity policies” that would function analogously to privacy policies.

DOI: <https://doi.org/10.15779/Z38TQ5RF73>.

© 2022 Dustin Marlan.

† Assistant Professor of Law, University of North Carolina School of Law. Many thanks to those who provided helpful comments on earlier drafts or at various conferences and workshops, including BJ Ard, Robert Fairbanks, Khash Goshtasbi, Jeremiah Ho, Anne Klinefelter, Saru Matambanadzo, Elizabeth McCuskey, Shalev Netanel, Alexandra Roberts, Jennifer Rothman, Shaun Spencer, Christian Turner, and Rebecca Tushnet. I take full responsibility for any remaining scholarly dystopia.

TABLE OF CONTENTS

I.	INTRODUCTION	804
II.	ORWELLIAN PRIVACY.....	812
	A. BRIEF PRIVACY OVERVIEW.....	813
	B. THE ORWELLIAN METAPHOR	815
III.	HUXLEYAN PUBLICITY	820
	A. BRIEF PUBLICITY OVERVIEW.....	820
	B. THE HUXLEYAN METAPHOR.....	824
	C. CELEBRITY PUBLICITY	829
	D. THE PLEASURABLE SERVITUDE	837
IV.	PUBLICITY’S BRAVE NEW WORLD.....	848
	A. MANIPULATIVE PUBLICITY	848
	1. <i>Autonomy and Dignity Concerns</i>	852
	2. <i>Political and Democratic Concerns</i>	853
	B. PUBLICITY POLICIES	855
	C. FIRST AMENDMENT BALANCE	860
V.	CONCLUSION.....	864

I. INTRODUCTION

There are two ways by which the spirit of a culture may be shriveled. In the first—the Orwellian—culture becomes a prison. In the second—the Huxleyan—culture becomes a burlesque.

Neil Postman¹

Our society often describes *privacy* problems using the dystopian metaphor of “Big Brother”—the figurehead of the totalitarian government in George Orwell’s classic novel *Nineteen Eighty-Four* (1984).² Understood through the

1. NEIL POSTMAN, AMUSING OURSELVES TO DEATH: PUBLIC DISCOURSE IN THE AGE OF SHOW BUSINESS 155 (1985).

2. See, e.g., DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 31 (2006) (“Big Brother dominates the discourse of information privacy”) [hereinafter SOLOVE, THE DIGITAL PERSON]; Neil Richards, *The Danger of Surveillance*, 126 HARV. L. REV. 1934, 1948 (2013) (“Of course, the most famous cultural exploration of the conforming effects of surveillance is Orwell’s harrowing depiction in *Nineteen Eighty-Four* of the totalitarian state personified by Big Brother.”); Lora Kelley, *When “Big Brother” Isn’t Scary Enough*, N.Y. TIMES (Dec. 2019), <https://www.nytimes.com/2019/11/>

Orwellian metaphor—and particularly the “Big Brother is Watching You” maxim—privacy rights are forcefully invaded by the government’s constant use of surveillance and the unauthorized disclosures of personal information. Big Brother reflects the unease, inhibition, and self-censorship individuals feel in their private lives when at the mercy of a malevolent watcher.³ In this way, Big Brother serves as a helpful conceptual warning about the consequences of government abuse of power, privacy, and surveillance made possible through sinister implementation of high technology coupled with nefarious intent.⁴

Yet, our other personality right,⁵ the right of *publicity*, still lacks an appropriate metaphor, making it difficult to conceptualize, and thus to regulate effectively.⁶ The right of publicity is “the inherent right of every human being to control the commercial use of his or her identity.”⁷ This Article suggests that the problems with a commercially transferable right of publicity can be usefully analogized not to *1984* but rather to another chilling and well-known dystopia: Aldous Huxley’s *Brave New World*.⁸

04/opinion/surveillance-big-brother.html (“In terms of usage, ‘1984’ and Big Brother stomp other surveillance metaphors”); Carl S. Kaplan, *Kafkaesque? Big Brother? Finding the Right Literary Metaphor for Net Privacy*, N.Y. TIMES (Feb. 2001), <https://www.nytimes.com/2001/02/02/technology/kafkaesque-big-brother-finding-the-right-literary-metaphor-for.html> (“It’s customary these days for many legal thinkers, journalists and just plain civilians to use the phrase ‘Big Brother’ when bemoaning the loss of privacy . . .”).

3. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1398 (2001) [hereinafter Solove, *Privacy and Power*].

4. See generally GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

5. See, e.g., Jonathan Kahn, *Bringing Dignity Back to Light: Publicity Rights and the Eclipse of the Tort of Appropriation of Identity*, 17 CARDOZO ARTS & ENT. L. J. 213, 214 (1999) (referring to privacy and publicity as “the conjoined twins of our modern media-saturated society.”).

6. See, e.g., Rebecca Tushnet, *A Mask That Eats into the Face: Images and the Right of Publicity*, 38 COLUM. J.L. & ARTS 157, 158 (2015) (referring to the right of publicity as “conceptually unbounded”); Eric E. Johnson, *Disentangling the Right of Publicity*, 111 NW. U. L. REV. 891, 893 (2017) (noting that “courts have yet to clearly articulate what the right of publicity is”); Thomas E. Simmons, *An Estate Plan for Kanye West*, 39 CARDOZO ARTS & ENT. L. J. 1, 4 (2021) (explaining that the right of publicity “is usually defined in the negative sense—that is, not in terms of the use one may make of it, but in terms of the right to prohibit others from using it.”).

7. 1 J. THOMAS MCCARTHY & ROGER E. SCHECHTER, THE RIGHTS OF PUBLICITY AND PRIVACY § 1:3 (2d ed. 2019). The right of publicity is a state law right, having never been codified federally. In litigation, its elements generally include some version of: (1) standing to sue, meaning that plaintiff is the owner or licensee of the identity in question; (2) defendant has made a commercial use of one or more aspects of that identity; (3) plaintiff did not consent to the appropriation; and (4) the appropriation of identity resulted in harm—typically of an economic nature—to the plaintiff. *Id.*

8. See generally ALDOUS HUXLEY, BRAVE NEW WORLD (Harper Crest Library 1946) (1937).

Huxley wrote *Brave New World* as an expression of the anxiety of losing one's individual identity in a technology-driven future.⁹ In the novel, Huxley envisioned a utilitarian society gone awry, controlled through technological manipulation, conspicuous consumption, social conditioning, drug use, and entertainment addiction. In contrast to Orwell's Big Brother's forceful coercion, pacified citizens in Huxley's "World State" society willingly participate in their own servitude.¹⁰ Their lack of freedom and identity is reflected in the World State's hypnopædic proverb: "Every one belongs to every one else."¹¹

Commentators often consider the major problem with publicity rights to be the protection of rich and famous celebrities at the expense of the free expression of others who seek to exploit their personas as a matter of public discourse.¹² In celebrity-focused publicity cases, courts haphazardly prioritize celebrities' publicity rights over creators' First Amendment rights to free expression in exploiting celebrity personas for use in creative or newsworthy endeavors.¹³ As two leading commentators put it, the right of publicity's

9. See Bob Barr, *Aldous Huxley's Brave New World—Still a Chilling Vision After All These Years*, 108 MICH. L. REV. 847, 849 (2010).

10. See Daphne Jong, *Civilization and its (Dys)contents: Savagery, Technological Progress and Capitalism in Industrial and Information Dystopias*, INTERSECT Vol. 12 No. 3 (2019); Solove, *Privacy and Power*, *supra* note 3, at 1422.

11. HUXLEY, *supra* note 8, at 46, 50, 55, 142, 151, 245.

12. See, e.g., DAVID L. HUDSON, JR., PROTECTING IDEAS 88 (2006) ("The right of publicity threatens First Amendment values by punishing individuals for the content of their creations. Celebrities have used the right of publicity as a cudgel, hammering expression from the public domain."); Tushnet, *A Mask That Eats*, *supra* note 6, at 157 ("[C]ourts have allowed the right of publicity to etch into the First Amendment in their eagerness to reward celebrities for the power of their 'images' and to prevent other people from exploiting those images."); Thomas E. Kadri, *Drawing Trump Naked: Curbing the Right of Publicity to Protect Public Discourse*, 79 MD. L. REV. 899, 958 (2019) ("The time has come to curb the right of publicity and reframe the First Amendment justifications that face off against it . . . the tort censors—or at least ransoms—the portrayal of real people and threatens public discourse."); Stephen McKelvey et al., *The Air Jordan Rules: Image Advertising Adds New Dimension to Right of Publicity-First Amendment Tension*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 945, 954 (2016) (examining the right of publicity's expansion as contributing to its increasing tension with the First Amendment).

13. Tushnet, *A Mask that Eats*, *supra* note 6, at 158–59; see also Kadri, *Drawing Trump Naked*, *supra* note 12, at 909; cf. STACEY DOGAN, HAELAN LABORATORIES V. TOPPS CHEWING GUM: PUBLICITY AS A LEGAL RIGHT, INTELLECTUAL PROPERTY AT THE EDGE: THE CONTESTED CONTOURS OF IP 17, 20 (Rochelle Cooper Dreyfuss & Jane C. Ginsburg, eds., 2014) ("[W]hile courts often rule in favor of defendant on First Amendment grounds, they do so by applying murky legal standards that offer little certainty or comfort to parties thinking about selling a product that draws upon a celebrity's identity."). But see Reid K. Weisbrod, *A Copyright Right of Publicity*, 84 FORDHAM L. REV. 2803, 2812 (2016) (noting that courts often side with free expression over publicity rights, particularly as compared to copyright).

“jagged and unpredictable reach chills speech in extensive and immeasurable ways.”¹⁴

However, as some, such as publicity luminary Jennifer Rothman, have recently pointed out, the right of publicity can and should function as a vehicle for protecting the identity of everyday citizens in our digital age.¹⁵ Indeed, the high-profile lawsuits launched by celebrities to protect the unauthorized uses of their personas, while visible because they get litigated, are not commonplace.¹⁶ There are roughly eighteen of these “privileged” publicity decisions published per year in the United States, and a halo of filings and informal disputes surely extending far beyond that.¹⁷ Far more common, though, is the right of publicity’s “dark matter,”¹⁸ which is not litigated but refers to the constant contractual loss of identity (i.e., publicity) rights for

14. Robert C. Post & Jennifer E. Rothman, *The First Amendment and the Right(s) of Publicity*, 130 YALE L. J. 86, 91 (2020).

15. See JENNIFER E. ROTHMAN, *THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD* 183 (2018) (“Distinctions between public and private figures make little sense today as so-called private figures increasingly live public or quasi-public lives on . . . online fora.”) [hereinafter ROTHMAN, *RIGHT OF PUBLICITY*]. See also Dustin Marlan, *Unmasking the Right of Publicity*, 71 HASTINGS L. J. 419, 473 (2020) (“[R]ecasting the right of publicity through an intersubjective lens might allow the right to contribute to the development of not just the self, but of digital relationships and community—a far cry from publicity’s commonly held stereotype as a hedonic vehicle bolstering the rights of already wealthy celebrities and trampling on the First Amendment.”); Note, Noa Dreymann, *John Doe’s Right of Publicity*, 32 BERKELEY TECH. L.J. 673, 709 (2017) (“Seeing as eighty-one percent of Americans in the United States have a social media profile, non-celebrities are now more vulnerable than ever to having their identities appropriated.”); Note, Barbara Bruni, *The Right of Publicity as Market Regulator in the Age of Social Media*, 41 CARDOZO L. REV. 2203, 2207 (2020) (suggesting “that the right of publicity can be a useful tool for ordinary people to gain more control and bargaining power over their online personas”).

16. See *Right of Publicity*, FINDLAW (May 26, 2016) <https://corporate.findlaw.com/litigation-disputes/right-of-publicity.html> (“It should not be surprising that most cases involving right of publicity claims involve celebrities or public personalities; however, this is probably more a condition of the economics of litigation than the legal rights involved.”); see also Rebecca J. Rosen, *Something Like 0.0086 the World is Famous*, THE ATLANTIC, <https://www.theatlantic.com/technology/archive/2013/01/something-like-00086-of-the-world-is-famous/267397/>.

17. Dustin Marlan, “Published Decisions Based on Westlaw Key Number Searches in Right of Publicity, Trademark, Copyright, and Patent 2010-2021” (2022), available at https://scholarship.law.umassd.edu/fac_pubs/238/ (comparing results of Westlaw key number searches in Right of Publicity (379 K383-409), Trademark (382 K1000-1800), Copyright (99 K220-1202), and Patent (291 K401-2094) for the years 2010 to 2021)).

18. See Brian L. Frye, *Literary Landlords in Plaguetime*, 10 NYU J. IP & ENT. L. 225, 232 (2021) (referring to non-litigated occurrences of copyright appropriation as copyright’s “dark matter”). Frye might have preferred, though, that his work was not cited in this regard. See Brian L. Frye, *Plagiarize this Paper*, 60 IDEA 294 (2020) (advocating for the benefits of plagiarism in certain academic contexts).

hundreds of millions of individuals in the United States, and billions worldwide,¹⁹ on the internet and social media.²⁰

The Huxleyan metaphor—particularly through the “[e]very one belongs to every one else” proverb—captures the right of publicity’s application beyond celebrity, in this regard. As one court remarked, “[i]n a society dominated by reality television shows, YouTube, Twitter, and online social networking sites, the distinction between a ‘celebrity’ and a ‘non-celebrity’ seems to be an increasingly arbitrary one.”²¹ In capturing a society subjugated by social conditioning and technological manipulation, the Huxleyan metaphor reflects the (allegedly) consensual sacrifice of publicity rights our own citizens regularly encounter.

This transfer of identity occurs through the unregulated licensing of publicity rights on the internet and social media. Social media users²²—often by way of clickwrap or browsewrap terms of service agreements—voluntarily or unknowingly relinquish rights in their identities to social networks in exchange for the pleasures and comforts of digital worlds.²³ The emblematic social media cases involving the right of publicity thus far include *Cohen v. Facebook*, *Fralely v. Facebook*, *Perkins v. LinkedIn*, *Parker v. Hey, Inc.*, and *Groupon v. Dancel*, where internet platforms harvested social media users’ names and

19. The Article does not make any claims as to the applicability of publicity licenses outside of the United States and U.S. law.

20. According to a recent study from Statista, Facebook has approximately three billion active users worldwide. *Number of monthly active Facebook users worldwide as of 4th quarter 2021*, STATISTA <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> (last visited Apr. 4, 2022). This includes roughly 300 million social media users in the United States, or roughly two-thirds of the U.S. population. *Number of Facebook users in the United States from 2017 to 2026*, STATISTA <https://www.statista.com/statistics/408971/number-of-us-facebook-users/> (last visited Apr. 4, 2022).

21. *Fralely v. Facebook, Inc.*, 830 F. Supp. 2d 785, 808 (N.D. Cal 2011); see ROTHMAN, RIGHT OF PUBLICITY, *supra* note 15, at 183 (2018) (“Distinctions between public and private figures make little sense today as so-called private figures increasingly live public or quasi-public lives on . . . online fora.”).

22. While I will grudgingly use the term “user” in the social media context, it appears disparaging and objectifying in a similar manner as “consumer” does in trademark law. See generally Dustin Marlan, *Is the Word “Consumer” Biasing Trademark Law?*, 8 TEX. A&M L. REV. 367 (2021); Dustin Marlan, *Rethinking Trademark Law’s “Consumer” Label*, 55 GONZ. L. REV. 422 (2020).

23. See *Cohen v. Facebook, Inc.*, 798 F. Supp. 2d 1090, 1092 (N.D. Cal. 2011) (“As a ‘social networking’ internet site, Facebook exists because its users *want* to share information.”). More broadly, this lack of consent issue is well documented in the context of the internet and social media terms of service and privacy policies. See, e.g., MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 12 (2014); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013) [hereinafter Solove, *Consent Dilemma*]; *infra* Section III.D.

images and used them in connection with targeted advertisements and endorsements.²⁴

In response to these lawsuits, several prominent social networks have added or modified exculpatory provisions to their terms of service agreements. These publicity-related provisions take a broad license of users' rights of publicity, for purposes of endorsement-related advertising, in exchange for use of their platforms. Thus, because consent functions as a complete defense to a right of publicity claim, social networks must be strategic in crafting their terms of service to obtain the express consent of their users.²⁵ This Article labels this online "stripping away" of individuals' publicity rights through online contracts as the "pleasurable servitude," and explores it as a problem of online manipulation deserving of regulatory reform.²⁶ More broadly, the pleasurable servitude is emblematic of what Shoshana Zuboff labels surveillance capitalism.²⁷

The pleasurable servitude can be defined as the mandatory release of some control by social media users over their publicity rights, in return for the benefits of accessing digital worlds. As an example of the phenomenon, consider that, as a prerequisite for using the popular messaging app, all Snapchat users must "consent" to Snap Inc.'s terms of service, which grants

24. Cohen, 798 F. Supp. 2d 1090 (N.D. Cal. 2011) (concerning endorsements regarding the "Friend Finder" service); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011) (concerning targeted endorsements regarding "Sponsored Stories"); *Perkins v. LinkedIn*, 53 F. Supp. 3d 1222 (N.D. Cal. 2014) (regarding marketing with "Add Connections" tool); *Parker v. Hey, Inc.*, Case No. CGC-17-556257, 2017 Cal. Super. LEXIS 609 (Super. Ct. Cal. Apr. 14, 2017) (concerning name's used in connection with Twitter's text invitations sent to contacts); *Dancel v. Groupon, Inc.*, No. 18 C 2027, 2019 U.S. Dist. LEXIS 33698 (N.D. Ill. Mar. 4, 2019) (regarding Groupon's collection of public Instagram data to collect photos and use them in connection with targeted advertisements); *cf. Dobrowolski v. Intelius, Inc.*, No. 17 CV 1406, 2017 U.S. Dist. LEXIS 138587 (N.D. Ill. Aug. 29, 2017) (regarding Intelius and Instant Checkmate's use of plaintiff's name in search engine advertisements).

25. See, e.g., Cydney Tune & Lori Levine, *The Right of Publicity and Social Media: A Challenging Collision*, LICENSING J., at 16 (June/July 2015).

26. Online manipulation can be defined as "the ability of data collectors to use information about individuals to manipulate them." Daniel Susser, Beate Roessler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV. 1 (2019); see also Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 995 (2014) (explaining that technology companies purposely exploit the cognitive limitations of consumers in the digital context); Shaun B. Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959, 969 (2020) (explaining that "terms of service can also exploit consumer biases and vulnerabilities.").

27. SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* 8 (2019) (arguing that we have entered a new era of "surveillance capitalism" that operates by "unilaterally claim[ing] human experience as free raw material for translation into behavioral data," and then processing the data to "anticipate what [individuals] will do now, soon, and later.").

Snap an unrestricted, worldwide, royalty-free, irrevocable, and perpetual right and license to use the name, likeness, and voice, of anyone featured in [uploaded] Public Content for commercial and non-commercial purposes.”²⁸ Similar broad publicity license or waiver provisions exist on internet platforms including Facebook, TikTok, YouTube, Instagram, and Groupon.²⁹ On these and other platforms, users of social media “voluntarily relinquish some control over their personal information, in return for the benefits these websites provide, often free of charge.”³⁰

In *Brave New World*, terror is no longer necessary because people have become so deeply conditioned to love their servitude. As media theorist Neil Postman writes in the seminal *Amusing Ourselves to Death: Public Discourse in the Age of Show Business*, “in Huxley’s vision, no Big Brother is required to deprive people of their autonomy . . . people will come to love their oppression, to adore the technologies that undo their capacities to think.”³¹ Today, with the gravitating power of digital media, technology corporations are able to gain control of the identities of millions or billions of people. These social media users, willingly or perhaps because they are too distracted to notice, license their publicity rights to internet platforms, who, in turn, sell their users’ identities to advertisers as commodities.³² Such publicity transfer gone awry is not a dreary Orwellian totalitarianism but rather like a Huxleyan world of pleasure-seeking, technological manipulation, and socially conditioned alienation of identity.³³

The *Brave New World* analogy is not purely academic or literary. It is intended to be a useful rhetorical device in highlighting the right of publicity as a right belonging to everyone, not just celebrities, and the injustice of publicity rights’ forced transfer from individuals to internet platforms. According to George Lakoff and Mark Johnson’s conceptual metaphor theory, a metaphor is a way of “understanding and experiencing one kind of thing in

28. *Terms of Service*, SNAP INC., <https://snap.com/en-US/terms> (last visited April 15, 2022).

29. See *infra* notes 260-277 and accompanying discussion.

30. Daniel B. Garrie, *CyberLife: Social Media, Right-of-Publicity and Consenting to Terms of Service*, Thomson Reuters (July 19, 2017), *CyberLife: Social Media, Right-of-Publicity and Consenting to Terms of Service* (legalexecutiveinstitute.com).

31. POSTMAN, *supra* note 1, at iii.

32. Melody Nouri, *The Power of Influence: Traditional Celebrity vs Social Media Influencer*, ADVANCED WRITING: POP CULTURE INTERSECTIONS 1 (2018) (“The use of social media platforms has grown exponentially in the last decade. From 2008 to 2018, the percentage of the U.S. population with a social media profile has grown from 10% to a whopping 77%.”).

33. See *infra* Section III.D.

terms of another.”³⁴ Daniel Solove, in proposing a Kafkaesque metaphor for information privacy, notes that “metaphors are tools of shared cultural understanding. Privacy involves the type of society we are creating, and we often use metaphors to envision different possible worlds, ones that we want to live in and ones that we don’t.”³⁵ Jurists, legislators, politicians, and academics often use conceptual metaphors to understand new surveillance technologies and their application to privacy laws.³⁶

Similarly, conceptual metaphors can be applied to online manipulation, surveillance capitalism, and the right of publicity. To this end, this Article proposes regulation regarding “publicity policies”—akin to privacy policies—that emphasize, rather than bury, mandated disclosures of appropriation of users’ commercial identities—name, image, and likeness—on websites across the internet and social media.³⁷ Inherent in these publicity policies should be publicity settings, including options to opt-out of, or customize, the internet platform’s use of one’s identity for advertising, marketing, and endorsements.³⁸ This sort of “publicity self-management” will not alone solve the problem³⁹ but is intended to serve as a realistic first step in drawing attention to the issue and therefore toward preventing this sort of mass identity alienation.

The Article proceeds as follows. In setting the stage for a Huxleyan right of publicity discussion, Part II gives an overview of the Orwellian metaphor for privacy problems. Section II.A provides background regarding privacy’s evolution from Warren and Brandeis’s historical “right to be left alone” to our current “age of surveillance.” Section II.B examines the Orwellian conception

34. GEORGE LAKOFF & MARK JOHNSON, *METAPHORS WE LIVE BY* 5 (1980); *see also* Dustin Marlan, *Visual Metaphor and Trademark Distinctiveness*, 93 WASH. L. REV. 767, 778 (2018) (applying conceptual metaphor theory in the trademark and advertising context and noting that “the focus of metaphor . . . is on understanding how one idea or concept can be understood in terms of another one, i.e., ‘A is B.’”).

35. SOLOVE, *THE DIGITAL PERSON*, *supra* note 2, at 28; *see also* J.M. BALKIN, *CULTURAL SOFTWARE: A THEORY OF IDEOLOGY* 247 (1998) (explaining that “metaphoric models selectively describe a situation, and in doing so help to suppress alternative conceptions.”); Lauren Henry Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 TENN. L. REV. 863, 871 (2018) (“Lawyers use applied analogies to understand and address specific problems in the law.”).

36. *Id.*; *see infra* Sections II.B and II.C.

37. *See infra* Section IV.A.

38. *Id.*

39. Solove, *Consent Dilemma*, *supra* note 23, at 1880 (acknowledging that “privacy self-management is certainly a laudable and necessary component of any regulatory regime” but is also “being tasked with doing work beyond its capabilities”); *see also* WOODROW HARTZOG, *PRIVACY’S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* 21 (2018) (explaining that “all the focus on [user] control distracts you from what really affects your privacy in the modern age.”).

of privacy breach as one involving Big Brother, the malevolent watcher, reflective of power and control by overreaching government actors.

Part III provides an analogous Huxleyan conceptualization of the right of publicity. Section III.A offers background on the right of publicity and its modern function as a transferable (i.e., licensable) intellectual property right. Section III.B provides an overview of *Brave New World* and its potential as a metaphor for publicity problems. Section III.C applies the Huxleyan metaphor to the celebrity-oriented aspect of the right of publicity, and Section III.D extends the metaphor to the online publicity licensing phenomenon—what this Article labels the “pleasurable servitude.”

Part IV charts a “brave new world” for the right of publicity. Section IV.A discusses the pleasurable servitude as a form of online manipulation—and, more broadly, of surveillance capitalism—and hence an autonomy, dignity, social, and political problem. Section IV.B proposes regulation in the form of “publicity policies.” Section IV.C contrasts First Amendment balancing considerations in the context of celebrity publicity—where noncommercial speech is often at stake—and the pleasurable servitude—which this Article argues should be seen purely as a matter of commercial speech, and thus outside the ambit of core historic First Amendment protection.

In conclusion, the Article reiterates its central thesis: if privacy law must be regulated, beyond the common law privacy torts, to respond to an Orwellian “Age of Surveillance,”⁴⁰ then publicity law, beyond the common law right of publicity, should be regulated to respond to a Huxleyan “Age of Instagram Face.”⁴¹

II. ORWELLIAN PRIVACY

*[The poster] depicted simply an enormous face, more than a meter wide: the face of a man about forty-five, with a heavy black mustache and ruggedly handsome features . . . BIG BROTHER IS WATCHING YOU, the caption beneath it ran.*⁴²

To set the stage for a parallel discussion of the Huxleyan right of publicity, this Part offers an overview of the Orwellian conception of privacy. The right to privacy is “[t]he principal historical antecedent of the right of publicity.”⁴³ This Part provides a brief historic overview of privacy and then discusses the

40. Richards, *The Dangers of Surveillance*, *supra* note 2, at 1936.

41. Jia Tolentino, *The Age of Instagram Face*, THE NEW YORKER (Dec. 12, 2019), <https://www.newyorker.com/culture/decade-in-review/the-age-of-instagram-face> (“How had I been changed by an era in which ordinary humans receive daily metrics that appear to quantify how our personalities and our physical selves are performing on the market?”).

42. ORWELL, *supra* note 4, at 2.

43. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 cmt. b (2008).

1984 metaphor and particularly the “Big Brother is watching you” motif as a central, if imperfect, framing for modern surveillance concerns, particularly in a post-9/11 era.⁴⁴

The sinister Big Brother metaphor captures the unease, inhibition, and self-censorship one feels in an era of total surveillance.⁴⁵ The Big Brother metaphor’s depiction of harm resulting from undue power and control at the hands of a malevolent watcher helps to justify an expansive notion of privacy—an ethereal personality right that is difficult to conceptualize in literal fashion.⁴⁶ Thus, finding the right metaphor is important in deciding how to regulate the area.⁴⁷ As demonstrated in later Parts, the use of conceptual metaphors is needed in the right of publicity context too.

A. BRIEF PRIVACY OVERVIEW

Samuel Warren and Louis Brandeis popularized the modern right of privacy in their 1890 Harvard Law Review article, *The Right to Privacy*.⁴⁸ In it, Warren and Brandeis advocate for a “right to be let alone,” and for the ability of every individual to determine “to what extent [their] thoughts, sentiments, and emotions shall be communicated to others.”⁴⁹ In echoing modern publicity concerns, Warren-Brandeis privacy was conceptualized, at least in part, to ward off unwarranted *publicity* stemming from the advent of new inventions and

44. See Deji Bryce Olukotun, *Sweep, Harvest, Gather: Mapping Metaphors to Fight Surveillance*, THE MILLIONS (Apr. 10, 2014), <https://themillions.com/2014/04/sweep-harvest-gather-mapping-metaphors-to-fight-surveillance.html> (“George Orwell’s novel 1984 continues to dominate literary metaphors with respect to surveillance.”); *supra* notes 2-4 and accompanying discussion.

45. See SOLOVE: THE DIGITAL PERSON, *supra* note 2, at 29.

46. See, e.g., WOODROW HARTZOG, PRIVACY’S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 10 (2019) (“Privacy is an amorphous and elusive concept.”); Calo, *Digital Market Manipulation*, *supra* note 26, at 1028 (“Distilling privacy harm is famously difficult.”).

47. See Kaplan, *supra* note 2. Information privacy is not the only legal subject area, though, where scholars have invoked dystopian literary metaphors. See, e.g., I. Bennett Capers, *Afrofuturism, Critical Race Theory, and Policing in the Year 2044*, 94 N.Y.U. L. REV. 1, 9 (2019) (employing Octavia Butler’s science fiction to imagine what policing might look like in the year 2044); Jennifer W. Reynolds, *Games, Dystopia, and ADR*, 27 OHIO ST. J. ON DISP. RESOL. 477, 482 (2012) (arguing “that modern alternative processes are just as susceptible to the dystopian inclinations that afflict the legal system, if not more so,” in providing a *The Hunger Games* metaphor for alternative dispute resolution).

48. See generally Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

49. *Id.* at 198.

technologies, such as the portable camera.⁵⁰ Although quaint by today's standards, such technology enabled new opportunities for commercial exploitation.⁵¹ In fashioning a "right to be let alone," Warren and Brandeis wrote that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life."⁵²

Warren-Brandeis' "right to be let alone" understands "privacy as a type of immunity or seclusion."⁵³ In this sense, privacy is a personal and nonassignable right protecting against psychic harm to thoughts, feelings, or emotions.⁵⁴ In distilling decades of privacy case law, prominent torts scholar William Prosser, in 1960, famously articulated the four "privacy torts"—(1) public disclosure of private facts; (2) intrusion on seclusion; (3) depiction of another in a false light; and (4) appropriation of another's image—the dignitary, privacy-rooted precursor to the commercial right of publicity.⁵⁵ Prosser's privacy torts have been accepted by nearly all U.S. courts, and were adopted in the Second Restatement of Torts.⁵⁶

50. Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 5-6 (1979) (noting that Warren, in particular, may have been especially concerned with unwanted publicity given that he was a member of high society frequently targeted by journalists).

51. Samantha Barbas, *From Privacy to Publicity: The Tort of Appropriation in the Age of Mass Consumption*, 61 BUFF. L. REV. 1119, 1120 (2013).

52. Warren & Brandeis, *supra* note 48, at 195.

53. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1808 (2010) (citing Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1101 (2002)).

54. Notable early privacy cases, which might be considered prototypical of modern publicity cases, minus the right of publicity's transferability, include *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 70 (Ga. 1905) (involving plaintiff's unauthorized endorsement for insurance); *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442, 442 (N.Y. 1902) (involving plaintiff finding her picture on an ad for Franklin Mills flour without permission); and *Edison v. Edison Polyform & Mfg. Co.*, 67 A. 392, 392 (N.J. Ch. 1907) (involving appropriation of Thomas A. Edison's name and likeness for use in labeling of pharmaceuticals); *O'Brien v. Pabst Sales Co.*, 124 F.2d 167, 168 (5th Cir. 1942) (involving use of famous football player's photograph on beer ad).

55. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 388-89 (1960).

56. Most relevant to the right of publicity, the Restatement definition of the tort of "Appropriation of Name and Likeness" is: "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of privacy." For a thorough comparison between the tort of appropriation and the right of publicity, see generally Kahn, *Bringing Dignity Back to Light*, *supra* note 5. Courts and commentators often sketch out a difference between the dignitary interests protected under the tort of appropriation and the commercial interests protected by the right of publicity. 1 J THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5:60 (1987) ("[I]nfringement of the right of publicity focuses upon injury to the pocketbook while an invasion of 'appropriation privacy' focuses upon injury to the psyche."); *People for the Ethical Treatment of Animals v. Berosini*, 895 P.2d 1269, 1283 (Nev. 1995) ("The appropriation tort seeks to protect an individual's personal interest in privacy . . . measured in terms of the mental anguish that

Yet, Warren-Brandeis privacy, as distilled into the four privacy torts, has proven inadequate to address the scope of modern privacy harms.⁵⁷ As Danielle Keats Citron writes, “[a]lthough twenty-first century technologies can similarly interfere with individual privacy, they magnify the harm suffered.”⁵⁸ Indeed, Warren and Brandeis could not have foreseen the exponential acceleration of technology which has led to the modern surveillance society. And Prosser’s four torts model has proved rigid and limiting.⁵⁹ Thus, in justifying enhanced regulations beyond the privacy torts, modern critiques of privacy rights in the information age frequently use the literary metaphor of George Orwell’s *1984* and its Big Brother motif to describe the evils of all-encompassing surveillance made possible by “an explosion of computers, cameras, sensors, wireless communications, GPS, biometrics, and other technologies.”⁶⁰

B. THE ORWELLIAN METAPHOR

What makes something “Orwellian”?⁶¹ George Orwell’s magnum opus, *1984*, provides a vocabulary to discuss surveillance, the police state, and authoritarianism, which includes terms like “thought police,” “telescreen,” “doublethink,” and, most famously, “Big Brother.”⁶² Big Brother, in particular,

results from the appropriation of an ordinary individual’s identity. The right to [sic] publicity seeks to protect the property interest that a celebrity has in his or her name.”) However, some states treat the two rights—appropriation and the right of publicity—interchangeably or recognize one or the other. For a comprehensive resource on state publicity laws, see Jennifer E. Rothman, *Rothman’s Roadmap to the Right of Publicity*, <https://www.rightofpublicityroadmap.com/>.

57. Neil M. Richards & Daniel J. Solove, *Prosser’s Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1889 (2010) (“Prosser bears at least some responsibility for the failure of the privacy torts to evolve in response to the technological and cultural developments of the last fifty years”).

58. Citron, *Mainstreaming*, *supra* note 53, at 1808.

59. Richards & Solove, *supra* note 57, at 1890.

60. “*Big Brother*” is no Longer a Fiction, *ACLU Warns in New Report*, ACLU (Jan. 15, 2003), <https://www.aclu.org/press-releases/big-brother-no-longer-fiction-aclu-warns-new-report>.

61. George Orwell, a pen name, was born Eric Arthur Blair (1903–1950). His other, numerous, politically-themed works include his first published book-length piece, *DOWN AND OUT IN PARIS AND LONDON* (1933) (depicting the theme of European poverty), *THE ROAD TO WIGAN PIER* (1937) (depicting 1930s depression-era London poverty), *THE LION AND THE UNICORN: SOCIALISM AND THE ENGLISH GENIUS* (1941) (critiquing Britain’s role in the Second World War), *POLITICS AND THE ENGLISH LANGUAGE* (1946) (essay criticizing the degradation of the English language, echoing his concept of Newspeak in 1984) and Orwell’s most famous work behind 1984, *ANIMAL FARM* (1945) (providing an allegory for Stalin’s Communist Russia).

62. Matthew Feeney, *Seventy Years Later, It’s Still “1984”* (June 5, 2019), <https://www.cato.org/commentary/seventy-years-later-its-still-1984> (claiming that “‘1984’ is at its

now serves as a “familiar metaphor that conjures up visions of political surveillance, political control of dissidents, totalitarian rule, and loss of individual liberty.”⁶³

Written in the late 1940s, *1984* describes a tyrannical state, Oceania, ruled by Big Brother—the figurehead of the totalitarian government.⁶⁴ As Orwell writes, “Big Brother is infallible and all-powerful . . . the guise in which the Party chooses to exhibit itself to the world.”⁶⁵ The Oceania government’s goal is “dreary conformity.”⁶⁶ To achieve this goal, Big Brother uses surveillance techniques resulting in fear and self-censorship: uniformed guards patrolling street corners, roving helicopters peer in from above, and a telescreen in every home “watches people as they watch it.”⁶⁷

Big Brother banned information to keep the public powerless, monitored its citizens every move, and enforced its brutal regime through the Gestapo-like Thought Police.⁶⁸ With Big Brother, “[t]here was of course no way of knowing whether you were being watched at any given moment.”⁶⁹ Orwell explains:

A Party member lives from birth to death under the eye of the Thought Police. Even when he is alone he can never be sure that he is alone. Whatever he may be, asleep or awake, working or resting, in his bath or in bed, he can be inspected without warning and without knowing that he is being inspected. Nothing that he does is indifferent. His friendships, his relaxations, his behavior toward his wife and children, the expression of his face when he is alone, the words he mutters in sleep, even the characteristic movements of his body, are all zealously scrutinized.⁷⁰

core a novel about language; how it can be used by governments to subjugate and obfuscate, and by citizens that resist oppression”).

63. Daniel J. Power, *“Big Brother” can watch us*, 25 J. DECISION SYS., 578, 578 (2016).

64. ORWELL, *supra* note 4, at 2.

65. ORWELL, *supra* note 4, at 2.

66. *See* Kaplan, *supra* note 2.

67. *See* Kaplan, *supra* note 2.

68. ORWELL, *supra* note 4, at 9 (“People simply disappeared, always during the night. Your name was removed from the registers, every record of everything you had ever done was wiped out, your one-time existence was denied and then forgotten.”). Not all citizens are heavily scrutinized, though, in *1984*. While the upper and middle classes (labeled “Party” members) are monitored intensely through telescreens and microphones, the lower classes (referred to as “Proles”) are presumed to be politically harmless and thus left to their own devices. ORWELL, *supra* note 4, at 24.

69. ORWELL, *supra* note 4, at 2.

70. ORWELL, *supra* note 4, at 99.

As a surveillance metaphor, Big Brother is one of power and control, which is achieved through the domination of one's inner, private life.⁷¹ For sociologist Dennis Wrong, “[t]he ultimate horror in Orwell’s imagined anti-utopia is that men are deprived of the very capacity for cherishing private thoughts and feelings opposed to the regime, let alone acting on them.”⁷²

Big Brother is an imperfect, but nonetheless effective, metaphor for our surveillance age. The metaphor concentrates our attention on local issues like police forces with traffic cameras to nationwide issues such as National Security Agency surveillance using massive databases.⁷³ As Daniel Power notes, a chief concern regarding government data collection “is its misuse to extend political ‘thought’ control.”⁷⁴ It is true that Orwell’s depiction of a conformist, totalitarian regime does not mirror our own private sector dominated “informational capitalism,”⁷⁵ as Julie Cohen refers to it. Yet, “Orwell’s insights about the effects of surveillance on thought and behavior remains valid—the fear of being watched causes people to act and think differently from the way they might otherwise.”⁷⁶ In this way, Big Brother serves as a conceptual warning for the dangers of government and private sector intrusion into one’s personal life and helps fashion privacy laws designed to combat these practices.⁷⁷

Of course, Big Brother is not the only effective metaphor for articulating privacy problems. Some view Big Brother as inadequate, including its failure to distinguish government surveillance from private sector surveillance. Several other metaphors have been conceptualized, though none have gained

71. See SOLOVE, THE DIGITAL PERSON, *supra* note 2, at 31 (“The metaphor of Big Brother understands privacy in terms of power, and it views privacy as an essential dimension of the political structure of society. Big Brother attempts to dominate the private life because it is the key to controlling an individual’s entire existence: her thoughts, ideas, and actions.”).

72. DENNIS WRONG, POWER: ITS FORMS, BASES AND USES 98 (1988).

73. See, e.g., *United States v. Howard*, 426 F. Supp. 3d 1247, 1249 (M.D. Ala. 2019) (referring to “twentieth century fears that Big Brother is watching” in the context of unreasonable search and seizure); Samuel D. Hodge, Jr., *Big Brother is Watching: Law Enforcement’s Use of Digital Technology in the Twenty-First Century*, 89 U. CIN. L. REV. 30 (2020); Note, Robert Fairbanks, *Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpenter*, 26 BERKELEY J. CRIM. L. 71, 72-73 (2021).

74. See Power, *supra* note 63, at 579 (2016).

75. See generally JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); see also Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460 (2019) (offering a comparison between Zuboff’s *The Age of Surveillance Capitalism* and Cohen’s *Between Truth and Power*).

76. Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1948 (2013).

77. See, e.g., California Consumer Privacy Act (CCPA), CA.GOV, <https://oag.ca.gov/privacy/ccpa>.

the platform of Orwell's Big Brother. And some are modifications of the Big Brother motif itself.⁷⁸

Shoshana Zuboff proposes the metaphor of “Big Other” to signify that a threat to our data privacy stems not only from a centralized government (i.e., Big Brother) but also a decentralized private sphere, which she labels “surveillance capitalism.”⁷⁹ William Staples uses the metaphor of “Tiny Brothers” to refer to “the quiet seemingly innocuous [surveillance] techniques that appear in the workplace, the school, the community and the home.”⁸⁰ Michel Foucault popularized Jeremy Bentham's panopticon as a metaphor for digital sensing and control, reminding us that everyone—not just the party members, as in 1984—is a potential surveillance target.⁸¹ Kevin Haggerty and Richard Ericson liken “the convergence of once discrete surveillance systems” to a “surveillant assemblage” in drawing from the post-structuralist landscape of Deleuze and Guattari's assemblage theory.⁸² Daniel Solove persuasively argues that the “helplessness, frustration, and vulnerability one experiences

78. See, e.g., Lora Kelley, *When 'Big Brother' Isn't Scary Enough*, N.Y. TIMES, (Nov. 4., 2019), <https://www.nytimes.com/2019/11/04/opinion/surveillance-big-brother.html>.

79. Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, *Journal of Information Technology*, 30 J. INFO. TECH. 75, 75-76, 82 (Mar. 2015) (“Unlike the centralized power of mass society, there is escape from Big Other. There is no place where Big Other is not.”).

80. William G. Staples, *How our culture of surveillance dictates our lives*, USA TODAY, <https://www.usatoday.com/story/cybertruth/2014/01/24/how-pervasive-surveillance-influences-how-we-live/4808699/> (discussing WILLIAM G. STAPLES, EVERYDAY SURVEILLANCE: VIGILANCE AND VISIBILITY IN POSTMODERN LIFE (2000)) (listing examples of “Tiny Brothers,” which contribute to a “culture of surveillance,” including employers' use of electronic monitoring of employee emails and internet usage, use of data mining techniques to pitch ads to consumers, and police scans and storage of license plate numbers).

81. See JEREMY BENTHAM, DEONTOLOGY; OR, THE SCIENCE OF MORALITY 100 (1834) (envisioning a circular wall of cells surrounded by a single guard tower—due to the building's unique design, the occupants cannot tell whether guards are occupying the tower or not, leading them to believe they are always under surveillance); MICHEL FOUCAULT, DISCIPLINE AND PUNISHMENT 201 (1977) (popularizing the panopticon metaphor for digital sending and control); Mason Marks, *Biosupremacy: Big Data, Antitrust, and Monopolistic Power*, 55 U.C. DAVIS L. REV. 513, 524 (2021) (describing the “digital panopticon [a]n engine for generating and exerting biopower because it enables platforms to monitor billions of people, calculate statistics on their physical and psychological traits, and nudge them to conform their behavior to norms established by the platforms.”).

82. Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. SOC. 605, 606 (2000) (“This assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct “data doubles” which can be scrutinized and targeted for intervention. In the process, we are witnessing a rhizomatic leveling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored.”).

when a large bureaucratic organization has control over a vast dossier of details about one's life" is more Kafkaesque than Orwellian.⁸³ And Noah Berlatsky finds that Philip K. Dick's science-fiction work provides a better comparison than Orwell to the reality of surveillance in our systemically racist society.⁸⁴ Berlatsky writes regarding the Phildickian metaphor:

Police profiling programs like stop and frisk are designed to give the authorities the power to regulate young Black and Hispanic men, while leaving others largely unmolested. Big Brother is watching you—but only if “you” fit certain criteria. Orwell doesn't capture that reality—but there are books that do. Philip K. Dick's 1968 *Do Androids Dream of Electric Sheep?*, for one, is set in a run-down future dystopia that is dilapidated rather than authoritarian. The protagonist, Rick Deckard, is a policeman, but he doesn't spy on his neighbors or terrorize the general populace. Instead, he is focused on identifying, tracking down, and destroying androids. The surveillance apparatus and the murderous force of the state are targeted, specifically, towards those defined as different.⁸⁵

In sum, Big Brother, as well as a host of other surveillance metaphors, are useful for depicting *privacy* problems. By contrast, our other personality right, the commercially oriented right of *publicity*, still lacks a suitable conceptual metaphor.⁸⁶ As one commentator puts it, “courts have yet to articulate what the right of publicity is.”⁸⁷ Moreover, the term “publicity,” like “privacy,” is itself a metaphor that—in connoting fame, celebrity, and stardom—may be obscuring our views about what a “right to identity” should consist of.

83. Solove, *Privacy and Power*, *supra* note 3, at 1421; see SOLOVE, THE DIGITAL PERSON, *supra* note 2, at 27-56 (providing a thorough literary analysis of the conceptual distinctions between Orwell's *1984* and Franz Kafka's *The Trial* as privacy metaphors). Moreover, Neil Richards explains that the term “privacy” is itself a metaphor. Richards notes that “the existing metaphors and conceptions—Big Brother, ‘invasion of privacy,’ the secrecy paradigm, and the public/private distinction—have become so engrained into our collective understanding that they dominate any discussion of something as ‘privacy.’” Therefore, using literal terminology like “data protection” or “confidentiality” has certain advantages when proposing new frontiers in this metaphor saturated area of the law. Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1135 (2006).

84. Noah Berlatsky, *Stop Comparing the NSA to 1984 (and Start Comparing It to Philip K. Dick)*, THE ATLANTIC (Apr. 9, 2014), <https://www.theatlantic.com/entertainment/archive/2014/04/stop-comparing-the-nsa-to-em-1984-em-and-start-comparing-it-to-philip-k-dick/360353/>.

85. *Id.*

86. See Marlan, *supra* note 15, at 448.

87. Johnson, *supra* note 6, at 891.

III. HUXLEYAN PUBLICITY

*Everybody belongs to every one else—don't they, don't they*⁸⁸

This Part theorizes a Huxleyan conceptualization of the right of publicity. It first provides background on publicity rights. This Part then discusses *Brave New World* and its potential as a metaphor for modern publicity problems. It next applies the *Brave New World* metaphor, particularly through the work of McLuhanesque media theorist Neil Postman, to the traditional notion of a celebrity-focused right of publicity. This Part lastly applies the Huxleyan metaphor to the modern online publicity licensing phenomenon. In analogizing to *Brave New World*, the Article labels the publicity license provisions in internet platforms' terms of service agreements the "pleasurable servitude."

A. BRIEF PUBLICITY OVERVIEW

The right of publicity "is an intellectual property right of recent origin which has been defined as the inherent right of every human being to control the commercial use of his or her identity."⁸⁹ Depending on the state law at issue, "identity" may include name, image, likeness, voice, signature, or other personally identifying traits.⁹⁰

Though the idea of a legal notion of publicity was not new (the right of publicity is similar doctrinally to the privacy tort of appropriation),⁹¹ the term "right of publicity" was ostensibly coined by Judge Jerome Frank in the seminal 1953 case *Haelan Laboratories v. Topps Chewing Gum*.⁹² In that controversial decision, Judge Frank stated:

88. HUXLEY, *supra* note 8, at 142.

89. *ETW Corp. v. Jireh Pub., Inc.*, 332 F.3d 915, 928 (6th Cir. 2003) (citing MCCARTHY, 1 THE RIGHTS OF PUBLICITY AND PRIVACY § 1:3) (2d ed. 2000)).

90. *See e.g.*, Alabama Code 1975 § 6-5-771(1), where Alabama's Right of Publicity Act defines "Indicia of Identity" broadly to "[i]nclude those attributes of a Person that serve to identify that Person to an ordinary, reasonable viewer or listener, including but not limited to, name, signature, photograph, image, likeness, voice, or a substantially similar imitation of one or more of those attributes." By contrast, Virginia's statute recognizes a narrower right to prevent the unauthorized use of one's "name, portrait, or picture . . . for advertising purposes or for the purposes of trade." Virginia Code § 8.01-40.

91. *See* ROTHMAN, RIGHT OF PUBLICITY, *supra* note 15, at 11-29 ("Concerns over the misappropriation of identity and unwanted publicity were not novel when the right of publicity purportedly emerged in the 1950s. To the contrary, they were long-standing and in large part the inciting incident for the development of the right of privacy itself.").

92. 1 MCCARTHY & SCHECHTER, *supra* note 7, § 1:26 ("Judge Jerome Frank was apparently the first to coin the term 'right of publicity.'"); *see also* Joseph R. Grodin, *The Right of Publicity: A Doctrinal Innovation*, 62 YALE L.J. 1123, 1124, 1126 (1953) ("[T]he Court of Appeals for the Second Circuit, speaking through Judge Frank, recently held that an individual has, independent of the right of privacy, rights in his name or picture which can be granted to

We think that in addition to and independent of that right of privacy (which in New York derives from statute), a man has a right in the publicity value of his photograph, i.e., the right to grant the exclusive privilege of publishing his picture, and that such a right may validly be made “in gross,” i.e., without an accompanying grant of a business or of anything else This right might be called a “right of publicity.”⁹³

In distinguishing publicity from privacy, Judge Frank noted that the right of publicity is both a right to prevent the commercial use of one’s identity as well as a *license* to grant use of that identity to a third party.⁹⁴

Judge Frank took the opportunity to fashion such a transferable right based on the unique facts of the *Haelan* case. The plaintiff, Haelan, a chewing gum manufacturer, obtained contracts with professional baseball players for the exclusive right to use their names and images in connection with baseball trading cards to be sold along with packs of chewing gum.⁹⁵ Defendant Topps, a rival chewing gum manufacturer, then used the same players’ names and images in connection with trading cards to be sold with their own gum.⁹⁶ Haelan sued to enjoin Topps’s use of the baseball players’ names and images on the trading cards.⁹⁷ In response, Topps argued that the baseball players had no legal right in their images (i.e., photos) other than the right of privacy, and one’s privacy right is strictly personal and thus cannot be assigned to others, such as Haelan.⁹⁸

In styling a remedy, Judge Frank, perhaps influenced by the psychoanalytic theories of his day—which bifurcated the public and private aspects of the personality—described a right distinct from privacy.⁹⁹ Although privacy rights

an exclusive licensee.... This new right of publicity allows a licensee of a famous person adequate protection against third parties.”); *cf.* Post & Rothman, *supra* note 14, at 93 n.22 (“What Frank and Nimmer added to the picture was the possibility that rights over one’s own identity could be transferable.”).

93. *Haelan Lab’s, Inc. v. Topps Chewing Gum, Inc.*, 202 F.2d 866, 868 (2d Cir. 1953).

94. *Id.* (explaining that one’s right of publicity is the “right to grant the exclusive privilege of publishing [his picture], and that such a grant may validly be made ‘in gross’”); *see also* § 10:53. 2 MCCARTHY & SCHECHTER, *supra* note 7, § 10:53 (“the holding in *Haelan* that an exclusive licensee has standing to sue has never been seriously questioned.”); Andrew Beckerman-Rodau, *Toward a Limited Right of Publicity: An Argument for the Convergence of the Right of Publicity, Unfair Competition and Trademark Law*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 132, 147-48 (2012) (explaining that the right of publicity is currently a property right that allows one to possess, use, exclude, and transfer their identity to others).

95. *Haelan*, 202 F.2d at 867.

96. *Haelan*, 202 F.2d at 867.

97. *Haelan*, 202 F.2d at 867.

98. *Haelan*, 202 F.2d at 867.

99. *See* Marlan, *Unmasking*, *supra* note 15, at 443–48.

are “rooted in the individual,” the right of publicity, governing the commercial identity and persona, is often alienable and descendible.¹⁰⁰ Far from a “right to be let alone,” the right of publicity is “anchored in commercial possibility.”¹⁰¹

In recognizing a transferable personality right, Judge Frank, in writing for the Second Circuit, ruled that the baseball players licensed Haelan a valid publicity right to their names and images.¹⁰² Thus, Haelan could recover against Topps in damages and receive injunctive relief for violation of its publicity right. As Jennifer Rothman puts it, the ball players are the “identity holders” who effectively transferred their publicity rights to Haelan as the “publicity holder.”¹⁰³ As a justification for such a right, Judge Frank claimed, quite thinly, that “it is common knowledge that many prominent persons (especially actors and ball-players), far from having their feelings bruised through public exposure of their likenesses, would feel sorely deprived if they no longer received money from authorizing advertisements, popularizing their countenances, displayed in newspapers, magazines, buses, trains, and subways.”¹⁰⁴

Seizing on Judge Frank’s description of this new transferable identity right, Melville B. Nimmer, soon after *Haelan*, wrote a law review article called *The Right of Publicity*.¹⁰⁵ In it, Nimmer identified two rationales for the right of publicity: “First, the economic realities of pecuniary values inherent in publicity, and second, the inadequacy of traditional legal theories protecting such publicity values.”¹⁰⁶ To these ends, Nimmer argued that the “right of publicity must be recognized as a property (not a personal) right, and as such capable of assignment and subsequent enforcement by the assignee.”¹⁰⁷

100. See, e.g., *Milton H. Greene Archives, Inc. v. CMG Worldwide, Inc.*, 2008 U.S. Dist. LEXIS 22213 (C.D. Cal. Jan. 7, 2008); *Lugosi v. Universal Pictures*, 603 P.2d 425 (1979); cf. Jennifer Rothman, *The Inalienable Right of Publicity*, 101 GEO. L. REV. 185 (2012) (exploring instances in which the right of publicity is not freely alienable and situating such alienability on a spectrum) [hereinafter Rothman, *Inalienable Right of Publicity*].

101. Mark Bartholomew, *A Right Is Born: Celebrity, Property, and Postmodern Lawmaking*, 44 CONN. L. REV. 301, 310 (2011).

102. *Haelan*, 202 F.2d at 868-69.

103. See Rothman, *Inalienable Right of Publicity*, *supra* note 100 at 187 (“The identity-holder is the person whose name, likeness, or other indicia of identity and, when used without permission, forms the basis of a right of publicity violation. The publicity holder, by contrast, is the person who owns the property interest in (commercial) uses of that identity.”).

104. *Haelan*, 202 F.2d at 868.

105. Melville B. Nimmer, *The Right of Publicity*, 19 LAW & CONTEMP. PROBS. 203, 204 (1954).

106. *Id.* at 215.

107. *Id.* at 216.

In the decades since, most states now recognize the right of publicity. About half of the states that recognize it have enacted statutory versions of the right of publicity, while the others continue to recognize the right at common law.¹⁰⁸ In 1976, the Supreme Court acknowledged a right of publicity in *Zacchini v. Scripps-Howard Broad. Co.*, where, despite the First Amendment, the Court recognized plaintiff Hugo Zacchini's right not to have his entire (fifteen second) "human cannonball" act broadcast on an Ohio local news channel (thus impacting the demand for ticket sales for the live act). From there, the right of publicity has continued to expand in scope.¹⁰⁹

In litigation, the right of publicity's elements typically require: (1) standing to sue (meaning that plaintiff is the owner or licensee of the identity in question); (2) defendant has made a commercial use of one or more aspects of that identity; (3) plaintiff did not consent to that appropriation; and (4) the appropriation of identity resulted in harm—usually of an economic nature—to plaintiff.¹¹⁰ From a transactional perspective, identity-holders, often celebrities, enter agreements to transfer their publicity rights to others, sometimes in exchange for vast compensation.¹¹¹ In transactional law, the right of publicity functions as a business asset.

Like Prosser did with the privacy torts, scholars have recently attempted to "disentangle" the various types of right of publicity cases into discrete categories. Eric Johnson proposes that the right of publicity consists of three dimensions: "(1) an endorsement right; (2) a merchandizing entitlement; and (3) a right against virtual impressment."¹¹² Robert Post and Jennifer Rothman offer four distinct publicity torts: "(1) the right of performance; (2) the right of commercial value; (3) the right of control; and (4) the right of dignity."¹¹³

Despite these efforts, courts and commentators continue to have difficulty conceptualizing right of publicity theory, policy, and doctrine. Eric Johnson likens the right of publicity's blackletter doctrine to "a large, shapeless block

108. See, e.g., CAL CIV. CODE § 3344.1; Illinois Right of Publicity Act (IRPA).

109. See, e.g., *Onassis v. Christian Dior-N.Y., Inc.*, 472 N.Y.S.2d 254, 260 (Sup. Ct. 1984) (explaining that the right of publicity has morphed into a free-standing, alienable property right protecting "the essence of the person, his or her identity or persona.").

110. 1 MCCARTHY & SCHECHTER, *supra* note 7, § 1:3.

111. See, e.g., Steve Olenski, "How Brands Should Use Celebrities For Endorsements," FORBES (July 20, 2016, 2:43 PM), <https://www.forbes.com/sites/steveolenski/2016/07/20/how-brands-should-usecelebrities-for-endorsements/#48a123e95593>. For example, LeBron James extended his original 9-year endorsement contract with Nike indefinitely, worth over a billion dollars over the course of James' lifetime. Cork Gaines, "Why LeBron James' record-breaking deal with Nike is a game-changer," BUS. INSIDER (Dec. 8, 2015, 9:41 PM), <https://www.businessinsider.com/lebron-james-nike-lifetimecontract-game-changer-2015-12>.

112. Johnson, *supra* note 6, at 891.

113. Post & Rothman, *supra* note 14, at 93-125.

of material.”¹¹⁴ Similarly, Thomas Simmons remarks that the right of publicity is “usually defined in the negative sense—that is, not in terms of the use one may make of it, but in terms of the right to prohibit others from using it.”¹¹⁵ Indeed, the right of publicity, as conceived of by Judge Frank, is notoriously elusive as a legal doctrine governing the ethereal identity, or persona.¹¹⁶ As with privacy, though, the right metaphor might shine a spotlight on previously hidden aspects of publicity and the harms associated with its transferability.

B. THE HUXLEYAN METAPHOR

What makes something “Huxleyan”?¹¹⁷ Aldous Huxley published *Brave New World* in 1932.¹¹⁸ The novel is, along with Orwell’s *1984*, “one of the two most widely discussed fantasies of this century.”¹¹⁹ *Brave New World* is a satire that depicts a utilitarian, scientifically perfected society premised on a caste system. Humans are operantly conditioned to occupy a place on the social hierarchy.¹²⁰

Huxley understood the power of technology not only to allow the government to control the population, like Big Brother, but also to manipulate through “artificial pleasures which dim the mind.”¹²¹ In differentiating the two novels, Huxley explained that “[i]n *1984*, the lust for power is satisfied by inflicting pain; in *Brave New World*, by inflicting a hardly less humiliating

114. Johnson, *supra* note 6, at 907.

115. Simmons, *supra* note 6, at 4.

116. See Jeffrey Malkan, *Stolen Photographs: Personality, Publicity, and Privacy*, 75 TEX. L. REV. 779, 829–35 (1997) (discussing the ambiguous nature of the term *persona* under right of publicity law); Marlan, *supra* note 15, at 426–429.

117. Aldous Huxley (1894–1963) is a well-known English writer and philosopher. Beyond *Brave New World*, Huxley wrote numerous novels and non-fiction works, including the utopian *Island* (1962), *Brave New World Revisited* (1958). Huxley is also well known for his work in mysticism including *The Perennial Philosophy* (1945) (illustrating commonalities between Western and Eastern mystical practices) and *The Doors of Perception* (1954) (interpreting his psychedelic experience with mescaline). For a legal perspective on psychedelic substances, see Dustin Marlan, *Beyond Cannabis: Psychedelic Decriminalization and Social Justice*, 23 LEWIS & CLARK L. REV. 851 (2019).

118. See generally HUXLEY, *supra* note 8. Both Huxley’s *Brave New World* and Orwell’s *1984* drew inspiration from the influential dystopia, Yvgeny Zamyatin, *We* (1924). See Paul Owen, *1984 Thoughtcrime? Does it Matter that George Orwell pinched the plot?*, THE GUARDIAN (2009), <https://www.theguardian.com/books/booksblog/2009/jun/08/george-orwell-1984-zamyatin-we>.

119. Rudolf B. Schmerl, *The Two Future Worlds of Aldous Huxley*, 77 PMLA 328, 328 (1962).

120. See 5 ALDOUS HUXLEY, COLLECTED ESSAYS 313 (1958).

121. Mario Varricchio, *Power of Images/Images of Power in Brave New World and Nineteen Eighty-Four*, 10 UTOPIAN STUDIES 98, 98 (1999).

pleasure.”¹²² Citizens are too distracted by “vapid pleasure, of mindlessness and numbness” to notice the chains that bind them.¹²³

Brave New World takes place hundreds of years in the future, in the year 632 AF (“After Ford”).¹²⁴ The settings are the “world zone” of “Central London,” representing the material world, and “The Reservation,” representing the primitive world.¹²⁵ The population, including protagonists Bernard Marx and Lenina Crowne, are kept docile through social conditioning, technological manipulation, and a narcotic called *soma*, which the government uses to sedate its people through an opiate-like euphoria.¹²⁶

The World State government is led by the benevolent dictator, Mustapha Mond, one of several “World Controllers,” who serves in mild-mannered contrast to the malevolent Big Brother.¹²⁷ Citizens in *Brave New World* are encouraged to take soma pills frequently, engage in promiscuous sex and conspicuous consumption, and use entertaining technologies such as television and virtual reality.¹²⁸ Such amusing distractions render the citizenry mindlessly content, politically passive, and culturally and intellectually vacuous.¹²⁹

Through these methods, the government keeps the population distracted enough not to realize that their personal freedoms are limited by a small elite who “combine complete control over social, political, and economic life with the achievement of material abundance.”¹³⁰ As Huxley describes in his later essay *Brave New World Revisited*, “non-stop distractions of the most fascinating nature . . . are deliberately used as instruments of policy, for the purpose of preventing people from paying too much attention to the realities of the social and political situation.”¹³¹

122. HUXLEY, *Brave New World Revisited* 27 (1958) [hereinafter HUXLEY, *REVISITED*].

123. Solove, *Privacy and Power*, *supra* note 3, at 1423.

124. HUXLEY, *supra* note 8, at 2.

125. Ahmed Ahmed Abdelaziz Farag, *Enslavement and Freedom in Aldous Huxley's Brave New World*, 7 *INT. J. ENG. & LIT.* 57, 59 (2015).

126. HUXLEY, *supra* note 8, at 52 (“The warm, the richly coloured, the infinitely friendly world of soma-holiday. How kind, how good-looking, how delightfully amusing every one was!”).

127. HUXLEY, *supra* note 8, at 52.

128. The one exception is John “the Savage,” who chooses to live on the Reservation.

129. Solove, *Privacy and Power*, *supra* note 3, at 1422.

130. Richard A. Posner, *Orwell versus Huxley: Economics, Technology, Privacy and Satire*, 24 *PHIL. & LIT.* 1, 14 (2000).

131. HUXLEY, *REVISITED*, *supra* note 122, at 43.

In blurring the lines between dystopia and utopia, the World State operates as a form of “pleasurable servitude.”¹³² As Judge Richard Posner writes, “[t]echnology has enabled the creation of the utilitarian paradise, in which happiness is maximized, albeit at the cost of everything that makes human beings interesting.”¹³³ Indeed, “the world of *Brave New World* enhances the role of technology and neglects the value of individuality.”¹³⁴

To deprive its citizens of identity and autonomy without the use of force, the World State government uses hypnopedia (i.e., sleep learning) techniques to brainwash its population. The hypnopædic mantra, “Every one belongs to every one else” is drilled into the minds of citizens from a young age.¹³⁵ As Mustapha Mond recites in the novel:

“But every one belongs to every one else,” [Mond] concluded, citing the hypnopædic proverb.

The students nodded, emphatically agreeing with a statement which upwards of sixty-two thousand repetitions in the dark had made them accept, not merely as true, but as axiomatic, self-evident, utterly indisputable.¹³⁶

When read literally, the “Every one belongs to every one else” slogan refers to the fact that monogamy and family rearing are not accepted in the World State—and promiscuity results in yet another pleasurable distraction from servitude.¹³⁷ More figuratively, the slogan perhaps symbolizes that no one is free, because everyone is subject to everyone else and, in effect, the property of everyone else. The World State’s inhabitants “are imprisoned in a predefined government mold, guided through carefully crafted and persistently enforced incentives.”¹³⁸ They “have no options, no free will, no chance to make a difference; only the opportunity to be another happy cog in a vast machine designed and run by the government.”¹³⁹

Through this pleasurable servitude, citizens in *Brave New World* sacrifice their identities, willingly or because they are too distracted to realize that they

132. *Aldous Huxley and Brave New World: The Dark Side of Pleasure*, ACAD. IDEAS (Jun. 21, 2018), <https://academyofideas.com/2018/06/aldous-huxley-brave-new-world-dark-side-of-pleasure/>.

133. Posner, *supra* note 130, at 13-14.

134. Farag, *supra* note 125, at 60.

135. HUXLEY, *supra* note 8, at 29, 31, 34, 81, 139.

136. HUXLEY, *supra* note 8, at 29.

137. HUXLEY, *supra* note 8, at 31.

138. Barr, *supra* note 9, at 856.

139. *Id.* at 856.

might have another option.¹⁴⁰ Huxley warns that this type of social conditioning becomes more effective as technology advances and there are greater insights as to the prediction and control of human behaviors.¹⁴¹ Huxley feared that a technology revolution would “bring each individual’s body, his mind, his whole private life directly under the control of the ruling oligarchy.”¹⁴² Such a “love of servitude cannot be established except as a result of a deep, personal revolution in human minds and bodies.”¹⁴³ In sum, “Orwell feared that what we hate will ruin us. Huxley feared that what we love will ruin us.”¹⁴⁴

There are at least two ways in which the right of publicity echoes *Brave New World*. In depicting a culture oppressed by an addiction to amusement and which uses entertainment as a form of control, the Huxleyan metaphor can be seen to reflect the overprotection of celebrities’ publicity rights at the expense of the First Amendment freedom of speech and expression of creators who seek to use these celebrity personas as part of their (otherwise) original works.¹⁴⁵ This encroachment on public discourse has negative ramifications for our democracy. As Neil Postman writes regarding the Huxleyan metaphor in *Amusing Ourselves to Death: Public Discourse in the Age of Show Business*:

When a population becomes distracted by trivia, when cultural life is redefined as a perpetual round of entertainments, when serious public conversation becomes a form of baby-talk, when, in short, a people become an audience and their public business a vaudeville act, then a nation finds itself at risk; culture-death is a clear possibility.¹⁴⁶

140. See HUXLEY, REVISITED, *supra* note 122, at 36 (noting that some who have advocated for a free society “failed to take into account man’s almost infinite appetite for distractions.”).

141. See HUXLEY, REVISITED, *supra* note 122, at 35.

142. GREGORY CLAEYS, *DYSTOPIA: A NATURAL HISTORY* 380 (2016).

143. HUXLEY, REVISITED, *supra* note 122, at xix (1958).

144. POSTMAN, *supra* note 1, at xx.

145. Compare POSTMAN, *supra* note 1, at 92 (“It is in the nature of the medium [television] that it must suppress the content of ideas in order to accommodate the requirements of visual interest; that is to say, to accommodate the values of show business.”), with Roberta Rosenthal Kwall, *Fame*, 73 IND. L. J. 1, 2 (1997) (“[O]ur obsession with fame and our reverence for celebrities have given rise to a unique [publicity] doctrine designed to protect against unauthorized attempts to utilize famous personas. Still, the doctrine presents something of an irony in that it provides increased economic protection for those who already are at this country’s top income level.”), and Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 CAL. L. REV. 127, 148 (1993) (noting that the influence of the cultural shift from a word-based to an image-based culture created a new form of celebrity eminence).

146. POSTMAN, *supra* note 1, at 155-56.

Perhaps, though, we might be too distracted by the rare celebrity publicity cases to realize that our own identities are constantly being appropriated.¹⁴⁷ Beyond celebrity, the Huxleyan metaphor—and especially the “[e]very one belongs to every one else” proverb—also captures the now widespread, but still overlooked, publicity problem the Article labels the “pleasurable servitude.” In effect, by consenting to clickwrap and browserwrap publicity licenses on the internet and social media, ordinary citizens literally transfer their identities in the form of broad publicity licenses to internet platforms. Thus, insights into the dystopian nature of an uncontrolled, transferable right of publicity, as applicable to ordinary citizens in our society, can be found in Huxley’s dark vision.

Under this analogy, social networking companies, like Facebook and Twitter, operate as “systems of governance”—or as Kate Klonick dubs them, our “New Governors.”¹⁴⁸ And social media platforms function as technological narcotics, a form of Brave New World’s soma.¹⁴⁹ In exchange for use of the platforms, internet users—like citizens of the World State—are conditioned through technology to forfeit legal rights to their identities.¹⁵⁰ And the mass scale of this identity transfer phenomenon echoes the “every one

147. See Noa Dreyman, *John Doe’s Right of Publicity*, 32 BERKELEY TECH. L.J. 673, 674 (2017) (suggesting that the right of publicity is meant not just for celebrities but for “every human being” and criticizing the Ninth Circuit for giving short shrift to a non-celebrity’s right to publicity in *Sarver v. Chartier*, 813 F.3d 891 (9th Cir. 2016)).

148. Klonick, *The New Governors*, 131 HARV. L. R. 1598, 1663 (2018) (“[t]he idea of governance captures the scope these private platforms wield through their moderation systems and lends gravitas to their role in democratic culture.”); see also Marks, *supra* note 81, at 516 (noting that social media platforms have “grown so powerful that their influence over human affairs equals that of many governments.”); Marjorie Heins, *The Brave New World of Social Media Censorship*, 127 HARV. L. REV. F. 325, 325 (2014) (explaining that, through its terms of service, Facebook wields more power, in terms of freedom of speech, than either monarchs or presidents).

149. See Chris Taylor, *Facebook Just Became the Ultimate Dystopia*, MASHABLE, (Jan. 12, 2018), <https://mashable.com/article/facebook-dystopia> (“[R]eplace ‘soma-holiday’ with ‘social media,’ and you can see why Huxley was even more prophetic than we’ve given him credit for.”).

150. See Rebecca MacKinnon, *If Not Orwell, Then Huxley: The Battle for Control of the Internet*, THE ATLANTIC (Feb. 9, 2012), <https://www.theatlantic.com/technology/archive/2012/02/if-not-orwell-then-huxley-the-battle-for-control-of-the-internet/252792/> (“In the Internet age, the greatest long-term threat to a genuinely citizen-centric society—a world in which technology and government serve instead of the other way around—looks less like Orwell’s *1984*, and more like Aldous Huxley’s *Brave New World*: a world in which our desire for security, entertainment, and material comfort is manipulated to the point that we all voluntarily and eagerly submit to subjugation.”).

belongs to every one else” proverb.¹⁵¹ Like in Huxley’s dystopia, individuals are conditioned to assign their identities to seemingly benevolent systems of governance. What do these digital governments do with the rights to its users’ (i.e., citizens’) identities? They sell them to advertisers as commodities for use in personalized, targeted advertisements.¹⁵²

The Huxleyan metaphor thus captures the right of publicity in its two-tiered nature—an extravagant, powerful celebrity right that has the potential to chill public discourse, but also one of servitude and dominion for the ordinary citizen who must voluntarily license their identity to maintain a normal relational or professional life or to feed their addiction to technology. Like *1984*, *Brave New World* is also an imperfect metaphor—it serves as a cartoonish exaggeration, rather than a realistic depiction, of surveillance capitalism. It is nonetheless helpful in showcasing the current and eventual harms of a commodified, licensable right in the identity. The next two Sections will apply the Huxleyan metaphor in greater detail to publicity’s two dimensions: (1) celebrity publicity and (2) the pleasurable servitude.

C. CELEBRITY PUBLICITY

This Section will apply the Huxleyan metaphor to the traditional, celebrity-focused right of publicity. The case law surrounding the right of publicity is overwhelmingly celebrity-centered. That is, famous people tend to be the ones who bring claims under the right of publicity. This is largely because of the economics of litigation—celebrities often can afford to do so, and their identities have market-based value, thereby making it easier to show the requisite commercial harm.¹⁵³ Though in many jurisdictions anyone can theoretically bring a right of publicity claim, many commentators frame the right of publicity as one “valuable mainly to celebrities.”¹⁵⁴ As Rebecca Rosenthal Kwall puts it in her article *Fame*, “our obsession with fame and our reverence for celebrities have given rise to a unique [publicity] doctrine designed to protect against the unauthorized attempts to utilize famous personas.”¹⁵⁵ Indeed, numerous celebrities have succeeded in using the right of publicity to stop others from appropriating their personas.

Paradigmatic examples include actress and singer Bette Midler succeeding in recovering damages from Ford Motor Company when a sound-alike of her

151. See generally *Right of Publicity*, ELEC. FRONTIER FOUND., <https://www EFF.ORG/issues/right-publicity> (last visited Apr. 18, 2022).

152. *Meta for Business*, META, (last visited Nov. 15, 2022) <https://www.facebook.com/business/tools/ads-manager>.

153. 1 MCCARTHY & SCHECHTER, *supra* note 7, § 1:3.

154. Richard A. Posner, *Misappropriation: A Dirge*, 40 HOUS. L. REV. 621, 634 (2003).

155. Kwall, *supra* note 145.

voice—singing her iconic single “Do You Want to Dance?”—was used on a Ford television commercial.¹⁵⁶ Johnny Carson was likewise able to recover against the defendant, Here’s Johnny Portable Toilets, Inc., when the company used his famous “Here’s Johnny” slogan along with the phrase “The World’s Foremost Comedian” in connection with its portable toilet products.¹⁵⁷ The musician, Don Henley, prevailed against department store Dillard’s, Inc. for appropriation of his name and likeness in connection with their advertisements for “henley” (three button) t-shirts (“Don loves his henley; you will too.”)¹⁵⁸ More recently, pop star Ariana Grande sued slumping fashion retailer Forever 21 for “publishing at least 30 unauthorized images and videos misappropriating [her] name, image, likeness, and music” in connection with an advertising campaign.¹⁵⁹

A dominant theoretical issue inherent in the celebrity publicity context is the right of publicity’s difficult balance with the First Amendment and, relatedly, the seeming lack of a sound justification for its existence.¹⁶⁰ As the late John Perry Barlow’s digital privacy and free expression-focused nonprofit organization, the Electronic Frontier Foundation, explains: “[r]ight of publicity cases raise important freedom of expression issues. When celebrities claim that a TV show or some other work violates their right of publicity, the cases effectively ask whether celebrities should have a veto right over creative works

156. *Midler v. Ford Motor Co.*, 849 F.2d 460 (9th Cir. 1988).

157. *Carson v. Here’s Johnny Portable Toilets, Inc.*, 698 F.2d 831, 832–33 (6th Cir. 1983).

158. *Henley v. Dillard Dep’t Stores*, 46 F. Supp. 2d 587, 589 (N.D. Tex. 1999)

159. *See Ariana Grande’s 10 Million Suit Against Forever 21 Has Been Set Aside, But the Fight is Far From Over*, THE FASHION L., (Nov. 12, 2019), <https://www.thefashionlaw.com/ariana-grandes-10-million-suit-against-forever-21-set-aside-but-the-fight-is-far-from-over/> (explaining that, given Forever 21’s bankruptcy status, the future of the right of publicity litigation is uncertain).

160. *See, e.g., Hart v. Elec. Arts, Inc.*, 808 F. Supp. 2d, 757, 774 (D.N.J. 2011), rev’d 717 F.3d 141 (3d. Cir. 2013) (noting that “no judicial consensus has been reached on the contours of the First Amendment vis-à-vis the right of publicity”); Mark Lemley and Stacy Dogan, *What the Right of Publicity Can Learn From Trademark Law*, 58 STAN. L. REV. 1161, 1162-63 (2006) (“[B]ecause the right of publicity rests upon a slew of sometimes sloppy rationalizations, courts have little way of determining whether a particular speech limitation is necessary or even appropriate in order to serve the law’s normative goals.”). Another related right of publicity issue is federal preemption, especially regarding the Copyright Act. *See, e.g., Jennifer E. Rothman, Copyright Preemption and the Right of Publicity*, 36 U.C. DAVIS L. REV. 199, 204 (2002) (“The right of publicity conflicts not only with explicit provisions of the Copyright Act, but also with the implicit grant of affirmative rights to copyright holders and the public, as well as with the purposes behind copyright protection.”); Rebecca Tushnet, *Raising Walls Against Overlapping Rights: Preemption and the Right of Publicity*, 92 NOTRE DAME L. REV. 153, 159 (2017) (“[C]omparing how preemption and First Amendment law have used purposive approaches to limit the right of publicity” and noting that “without a coherent justification for the right of publicity, there are no obvious stopping points for its scope.”)

that depict them.”¹⁶¹ In this regard, courts have struggled to develop a coherent test in balancing the right of publicity and the First Amendment.

Scholars have written at length about this frustrating balance and the negative implications of the right of publicity’s expansion at the expense of free expression.¹⁶² As Thomas Kadri writes regarding this perceived censorship in *Drawing Trump Naked*, “[i]n recent years, creators of expressive works have faced legal challenges from a bizarre cast of characters, including Panamanian dictator Manuel Noriega, Mexican drug lord ‘El Chapo’ Guzman, wayward actress Lindsey Lohan, and Hollywood dame Olivia de Havilland.”¹⁶³ Such creators provoked litigation by portraying real people.¹⁶⁴

The prevailing scholarly viewpoint is that the First Amendment serves as a virtuous limit on an out-of-control right of publicity.¹⁶⁵ This narrative ostensibly makes sense when the cases involve newsworthy public discourse, perhaps from the press or political speakers or artists.¹⁶⁶ But many publicity cases involve comparatively trivial subject matters, often a famous persona versus a corporate advertiser, where the First Amendment stakes are significantly lower given the commercial speech (i.e., advertising) at issue.¹⁶⁷ And the blanket emphasis on free speech over publicity rights does not take distributive justice concerns into account enough. As Steven Jamar and Lateef Mtima write, “[b]ecause of institutionalized barriers to information, financial capital, and legal support, many members of marginalized communities have been unable to commercially develop and exploit their publicity rights, while majority enterprises have proven quite adept at exploiting these properties.”¹⁶⁸

161. ELEC. FRONTIER FOUND., *supra* note 151.

162. *See* Kadri, *supra* note 13.

163. *See* Kadri, *supra* note 13, at 901.

164. *See* Kadri, *supra* note 13, at 901.

165. *See, e.g.*, Kadri, *supra* note 13, at 901; Post & Rothman, *supra* note 14; Tushnet, *supra* note 12; Eugene Volokh, *Freedom of Speech and the Right of Publicity*, 40 HOUS. L. REV. 903 (2003) (claiming that the right of publicity is “unconstitutional as to all noncommercial speech, and perhaps even as to commercial advertising as well”).

166. *See, e.g.*, Parks v. LaFace Recs., 329 F.3d 437 (6th Cir. 2003) (regarding legality of using civil rights icon Rosa Parks’ name without permission in hip-hop band Outkast’s song “Rosa Parks”); Winter v. DC Comics, 69 P.3d 473 (Cal. 2003) (involving comic book containing significant creative elements that transformed the celebrity identities depicted and were thus deserving of First Amendment protection).

167. *See infra* Section IV.C.

168. Steven D. Jamar and Lateef Mtima, *A Social Justice Perspective on Intellectual Property, Innovation, and Entrepreneurship*, Ch. 6 in MEGAN CARPENTER, ED., ENTREPRENEURSHIP AND INNOVATION IN EVOLVING ECONOMIES: THE ROLE OF LAW (ELGAR LAW AND ENTREPRENEURSHIP SERIES) 13 (2012).

The quintessential 1992 case *White v. Samsung Electronics America Inc.* epitomizes the “image as spectacle”¹⁶⁹ that is celebrity publicity. *White* involved a dispute between “Wheel of Fortune” host Vanna White who objected to an advertisement by Samsung for video cassette recorders. The ad depicting a robot dressed in a gown, wig, and jewelry, created to resemble White’s persona.¹⁷⁰ The caption for the ad read: “Longest-running game show. 2012 A.D.”¹⁷¹

White sued Samsung for depicting this roboticized version of her likeness without consent. The Ninth Circuit majority held in White’s favor on the right of publicity claim, finding that Samsung used White’s identity to its commercial advantage, without consent, resulting in economic injury to White.¹⁷² According to the Ninth Circuit:

The robot is standing on what looks to be the Wheel of Fortune game show set. Vanna White dresses like this, turns letters, and does this on the Wheel of Fortune game show. She is the only one. Indeed, defendant’s themselves referred to their ad as the “Vanna White” ad. We are not surprised. Television and other media create marketable celebrity identity value.¹⁷³

As a justification for protecting White’s right of publicity, the Ninth Circuit noted that “considerable energy and ingenuity are expended by those who have achieved celebrity value to exploit for profit.”¹⁷⁴ Publicity “law protects the celebrity’s sole right to exploit this value whether the celebrity has achieved her fame out of rare ability, dumb luck or a combination thereof.”¹⁷⁵

In a scathing dissent, then Chief Judge Alex Kozinski¹⁷⁶ famously wrote that overprotecting intellectual property is as dangerous as underprotecting

169. GUY DEBORD, *THE SOCIETY OF THE SPECTACLE* 144 (1967) (“The spectacle is capital accumulated to the point where it becomes image.”).

170. *White v. Samsung Elecs. Am. Inc.*, 971 F.2d 1395, 1396 (9th Cir. 1992).

171. *Id.*

172. *Id.* at 1399 (“The law protects the celebrity’s sole right to exploit [celebrity] value.”).

173. *Id.*

174. *Id.*

175. *Id.*

176. Kozinski retired in 2017 amid allegations of sexual harassment. Matt Zaposky, *Judge Who Quit Over Harassment Allegations Reemerges, Dismaying Those Who Accused Him*, WASHINGTON POST (Jul. 24, 2018), https://www.washingtonpost.com/world/national-security/judge-who-quit-over-harassment-allegations-reemerges-dismaying-those-who-accused-him/2018/07/23/750a02f2-89db-11e8-a345-a1bf7847b375_story.html; see Ixta Maya Murray, *Draft of a Letter of Recommendation to the Honorable Alex Kozinski, Which I Guess I’m Not Going to Send Now*, 25 MICH. J. GENDER & L. 59 (2018) (utilizing a legal-literary style to engage the jurisprudential moment of Kozinski’s resignation amidst the #MeToo movement).

it: “Parody, humor, irreverence are all vital components of the marketplace of ideas.”¹⁷⁷ Kozinski argues:

The panel’s opinion is a classic case of overprotection. Concerned about what it sees as a wrong done to Vanna White, the panel majority erects a property right of remarkable and dangerous breadth: Under the majority’s opinion, it’s now a tort for advertisers to remind the public of a celebrity. Not to use a celebrity’s name, voice, signature or likeness; not to imply the celebrity endorses a product; but simply to evoke the celebrity’s image in the public’s mind. This *Orwellian* notion withdraws far more from the public’s domain than prudence and common sense allow.¹⁷⁸

Judge Kozinski’s framing of the issue as “Orwellian” is notable. Vanna White is certainly a remarkable person.¹⁷⁹ But from a democratic perspective, *White v. Samsung* involves the balance between what amounts to a battle of distractions—a wealthy Hollywood star’s depiction as a robot by billionaire mega-corporation Samsung. In this way, the dilemma is fundamentally Huxleyan in nature, echoing the warnings of *Brave New World* more so than *1984*. Orwell’s *1984* warned about a tyrannical state that would ban information to keep the public powerless. By contrast, *Brave New World* depicted a culture too amused by distractions—entertainment, pleasure, and laughter—to realize that it had been made powerless by its ruling classes. In *Brave New World*, entertainment serves as a form of control, just as it does in our media-saturated society.

In 1985, media theorist Neil Postman warned that television posed a threat to liberal democracy given that corporations would be able to control the flow of public discourse and freedom of information through technology, and thus of cultural expression.¹⁸⁰ In channeling Marshall McLuhan’s concept of “the medium is the message,”¹⁸¹ Postman warned that “[t]elevision . . . is

177. *White*, 989 F.2d at 1514.

178. *White*, 989 F.2d at 1514 (emphasis added).

179. See, e.g., Aude Soichet and Alexa Valiente, *6,500 dresses later: ‘Wheel of Fortune’ host Vanna White on 35 years with Pat Sajak, why she loves her job*, ABC NEWS, (Oct. 30, 2017), <https://abcnews.go.com/Entertainment/6500-dresses-wheel-fortune-host-vanna-white-35/story?id=50819154>. For feminist jurisprudential critiques on *White v. Samsung*, see Emily Donohue, *White v. Samsung – Feminist Rewrite*, YOUTUBE (Apr. 22, 2020), https://www.youtube.com/watch?v=06_KIw1u4f8; Brian L. Frye, *Commentary on White v. Samsung*, in FEMINIST JUDGMENTS: REWRITTEN PROPERTY OPINIONS 149 (Eloisa C. Rodriguez Dod & Elena Maria Marty-Nelson eds., 2021), .

180. POSTMAN, *supra* note 1.

181. See generally Marshal McLuhan, *The Medium is the Massage*, in UNDERSTANDING MEDIA: THE EXTENSION OF MAN (1964). The spelling of “massage,” rather than message, is intentional, or at least purposely uncorrected in referring to a linguistic amalgamation of

transforming our culture into one vast arena for show business.”¹⁸² Postman writes:

What Huxley feared was that there would no reason to ban a book, for there would be no one who wanted to read one. Orwell feared those who would deprive us of information. Huxley feared those who would give us so much that we would be reduced to passivity and egoism. Orwell feared that the truth would be concealed from us. Huxley feared the truth would be drowned in a sea of irrelevance. Orwell feared we would become a captive culture. Huxley feared we would become a trivial culture, preoccupied with some equivalent of the feelies, the orgy porgy, and the centrifugal bumblepuppy.¹⁸³

As such, Postman suggests that we “look to Huxley, not Orwell, to understand the threat that television and other forms of imagery pose to the foundation of liberal democracy namely, to freedom of information.”¹⁸⁴ Indeed, “[i]n the Huxleyan prophecy, Big Brother does not watch us, by his choice. We watch him, by ours. There is no need for wardens or gates or Ministries of Truth.”¹⁸⁵

Disallowing Samsung Corporation the unlicensed right to use the persona of celebrity Vanna White on a television advertisement is not reminiscent of an Orwellian prison. Rather, it is more akin to a Huxleyan burlesque.¹⁸⁶ An ad featuring a robotic version of a game show host—by a court Judge Kozinski refers to as the “Hollywood Circuit”—echoes the Huxleyan triviality of culture rather than an Orwellian surveillance state where one’s private knowledge and expression is heavily restricted and controlled.

More specifically, the privileging of the Hollywood persona over the First Amendment is Huxleyan in the sense that our preoccupation with celebrity

“message,” “massage,” “mess age,” and “mass age.” See Dr. Eric McLuhan, *Commonly Asked Questions (and Answers)*, <https://www.marshallmcluhan.com/common-questions/>. Marshall McLuhan and Neil Postman, a McLuhan acolyte, were both influential in establishing the field now referred to as media ecology, “the study of media as environments.” See LANCE STRATE, *AMAZING OURSELVES TO DEATH: NEIL POSTMAN’S BRAVE NEW WORLD REVISITED* 24-30 (2014).

182. POSTMAN, *supra* note 1, at 80. According to Postman, Huxley “believed that it is far more likely that the Western democracies will dance and dream themselves into oblivion than march into it, single file and manacled.” Indeed, “Huxley grasped, as Orwell did not, that it is not necessary to conceal anything from a public sensible to contradiction, narcotized by technological diversions.” Thus, “spiritual devastation is more likely to come from an enemy with a smiling face than from one whose countenances exudes suspicion and hate.” POSTMAN, *supra* note 1, at 111.

183. POSTMAN, *supra* note 1, at vii-viii.

184. POSTMAN, *supra* note 1, at 155.

185. POSTMAN, *supra* note 1, at 156.

186. See POSTMAN, *supra* note 1, at 155.

persona—a television idol’s right of publicity—takes precedence over the “marketplace of ideas”—the free evocation of White’s image by others. In this way, the preference for protecting the value of amusement, entertainment, and celebrity, through a persona-focused right of publicity, chills the ability to engage in public discourse and the free exchange of ideas in a serious, civil, and respectful way.¹⁸⁷

This legal focus on protecting the value of entertainment via celebrity identity ostensibly leaves individuals ill-equipped to fulfill their obligations as citizens in a democracy. According to Alexander Meiklejohn’s influential justification of the First Amendment, the key purpose of free speech and expression is in preserving the open debate essential to democracy.¹⁸⁸ A celebrity-focused right of publicity has the potential to shut down this formation of public opinion.¹⁸⁹ Society prioritizes the exchange of images (i.e., personas) rather than the exchange of ideas (i.e., works of free expression based on those personas).¹⁹⁰ This legal emphasis reflects the passivity of culture depicted by Huxley in *Brave New World*.

As technology has evolved in recent decades, the subject matter of right of publicity cases has shifted to digital mediums beyond the playing cards of *Haelan*, and further still beyond *White’s* realm of game show television. Indeed, the scope of the right of publicity cases now encompasses synthetic recreations of personas.¹⁹¹ For Postman, when he wrote *Amusing Ourselves to Death* in the 1980s, television appeared as the all-encompassing form of media. A generation later, the internet has a far more pervasive influence than television, and Postman’s arguments appear a bit outdated in their focus on major

187. Yet the preference, at least as to these facts, does assist in preserving White’s subjective autonomy.

188. See, e.g., ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE 75 (1965) (claiming that the First Amendment’s “purpose is to give to every voting member of the body politic the fullest possible participation in the understanding of those problems with which the citizens of a self-governing society must deal.”); *Citizens United v. Fed. Election Comm’n*, 558 U.S. 310, 373 (2010) (stating that a “vibrant public discourse . . . is at the foundation of our democracy.”) (Roberts, J.).

189. See Tushnet, *supra* note 6, at 205–06 (“Celebrities, by concentrating our attention and interest, are good to think with . . . [C]elebrities offer important reference points enabling broader discussion.”).

190. See Tushnet, *supra* note 6, at 206 (“More serious attention to the communicative nature of images, as opposed to continued equation of an image with the person it represents, would lead to a substantial contraction of the right of publicity.”).

191. See, e.g., *Noriega v. Activision/Blizzard, Inc.*, BC 551747, 2014 WL 5930149, (Cal. Super. Ct., L.A. Cnty. Oct. 27, 2014) (involving former Panamanian dictator’s right of publicity claim based on depiction of his likeness in the *Call of Duty* videogame); *Kirby v. Sega of Am.*, 144 Cal. App. 4th 47, 51 (Cal. Ct. App. 2006) (involving singer Keirin Kirby’s right of publicity claim based on depiction of her likeness in the *Space Channel 5* videogame).

network television. But as media scholar Lance Strate—who wrote a follow-up to Postman’s book called *Amazing Ourselves to Death: Neil Postman’s Brave New World Revisited*—explains, “Huxley’s dystopia is also a society that worships technology in all of its forms.”¹⁹²

In cases involving digital recreations of personas, courts continue to struggle to balance the right of publicity with the First Amendment.¹⁹³ There is no uniform test for achieving this balance. However, the copyright fair use-derived transformative use test from *Comedy III Prod. Inc. v. Gary Saderup Inc.*¹⁹⁴ has come to prominence as the doctrinal mechanism for doing so in certain key jurisdictions, supplanting the trademark-like *Rogers v. Grimaldi* test.¹⁹⁵ Under the transformative use test, unauthorized use of an identity is permissible if the use adds significant creative elements and sufficiently transforms the identity into original expression.

In *No Doubt v. Activision Publishing*, for instance, members of the rock band No Doubt successfully sued video game publisher Activision, alleging that Activision’s recreations of band member likenesses exceeded the parties’ licensing agreement, violating their rights of publicity in the video game *Band Hero*.¹⁹⁶ Although No Doubt had agreed that Activision could develop digital avatars based on their personas, it had not agreed that the No Doubt avatars could play songs by other musical acts or alter Stefani’s vocals, as the game allowed.¹⁹⁷ Because the video game simulated what No Doubt did in real life—performing music concerts—the court held that Activision did not make a “transformative use” of No Doubt’s identities, and thus the right of publicity prevailed over the First Amendment.¹⁹⁸

Similarly, in *In re NCAA Student-Athlete Name & Likeness Licensing Litigation*, student-athletes prevailed in class action lawsuits based on use of their identities in Electronic Arts’ NCAA Football video game series, which featured the graphical representations of real-life college football players.¹⁹⁹

192. LANCE STRATE, *AMAZING OURSELVES TO DEATH: NEIL POSTMAN’S BRAVE NEW WORLD REVISITED* 12 (2014).

193. For a thorough recent commentary on calibrating the balance between the First Amendment and right of publicity, see generally Post & Rothman, *supra* note 14.

194. *See Comedy III Prods., Inc. v. Gary Saderup, Inc.*, 21 P.3d 797, 808 (Cal. 2001) (establishing the transformative use test in the right of publicity context).

195. *See Rogers v. Grimaldi*, 875 F.2d 994, 1005 (2d Cir. 1989) (establishing the “Rogers test”).

196. *No Doubt v. Activision Publ’g, Inc.*, 122 Cal. Rptr. 3d 397, 401-03 (2011).

197. *Id.*

198. *Id.* at 411.

199. *Keller v. Elec. Arts Inc.*, 724 F.3d 1268, 1289 (9th Cir. 2013). A similar case, also involving the NCAA football video game series, is *Hart v. Elec. Arts, Inc.*, 717 F.3d 141, 145-46 (3d Cir. 2013). For an analysis of the *Hart* and *Keller* cases, see James Kyper & Dustin

Because of NCAA restrictions, Electronic Arts did not license or compensate the players for use of their likenesses, nor did it ask for their consent prior to incorporating them into the video game.²⁰⁰

Similar to *No Doubt*, the court was persuaded that because the video game simulated college football, the players' likenesses were not sufficiently transformed to constitute highly original expression, and the players' rights of publicity thus trumped Electronic Arts' First Amendment rights. However, unlike other right of publicity cases, *In re NCAA Student Athlete* involved thousands of virtual actors, many of which were not famous in the conventional sense.²⁰¹ The lawsuit in this regard represents a departure from celebrity right of publicity cases. While a minority of the athletes represented might be considered major or minor celebrities, such as lead plaintiff Samuel Keller (then quarterback of Arizona State), the majority of college football players are not famous.

The right of publicity and its reconciliation with the First Amendment is thus an area that would benefit from much needed clarity. The Huxleyan metaphor reflects this Hollywood stifling of free expression given its focus on amusement and entertainment as a form of control. Yet there is a prevalent, but often overlooked, aspect to the right of publicity beyond celebrity: its application to ordinary citizens, particularly in the digital context. The Electronic Frontier Foundation (EFF) vows that it “will continue to work in this area to ensure that right of publicity claims are limited by robust free expression.”²⁰² But EFF also notes that “a limited version of this right [of publicity] makes sense” as “you should be able to prevent a company from running an advertisement that falsely claims that you endorse its products.”²⁰³ This two-tiered policy stance alludes to a dystopian world this Article calls the “pleasurable servitude.”

D. THE PLEASURABLE SERVITUDE

We might be too distracted by the celebrity publicity simulacrum²⁰⁴ to notice that our own identities are constantly being licensed to technology

Marlan, *When Does the Right of Publicity Trump a Video Game Maker's First Amendment Rights?*, 18 CYBERSPACE LAW. 11 (2013), <https://www.jdsupra.com/legalnews/when-does-the-right-of-publicity-trump-a-69233/>.

200. Keller, 724 F.3d at 1289.

201. Keller, 724 F.3d at 1289.

202. ELEC. FRONTIER FOUND., *supra* note 151.

203. ELEC. FRONTIER FOUND., *supra* note 151.

204. See generally JEAN BAUDRILLARD, SIMULACRA AND SIMULATION (1981) (referring to “simulation,” “simulacra,” and “hyperreality” as relating to manufactured representations of the world that appear more real than actual events because they are created for the media, made accessible through the media, and work within the biases established by the media).

corporations. In fact, celebrity publicity cases are not altogether common. There are very few celebrities in society relative to ordinary people.²⁰⁵ One estimate puts the figure at about 0.0265 percent of the U.S. population; another at 1 in 2,000 people.²⁰⁶ In terms of the whole world, the number of celebrities is far lower at 0.0086 percent.²⁰⁷

From 2015 to 2021, there were an average of roughly eighteen published right of publicity cases decided per year.²⁰⁸ Beyond these recorded cases, there are many more court filings and undoubtedly numerous informal disputes that are never litigated.²⁰⁹ Indeed, the inconsistency inherent in this legal area has the potential to chill free speech *ex ante*. But there is another, far more widespread aspect to the right of publicity that is also captured by the Huxleyan metaphor: publicity's application to ordinary citizens through the internet and social media.²¹⁰ By contrast to celebrity publicity, as of 2020, Facebook has over 2.85 billion users worldwide and over 231 million users just in the United

205. Though that number has likely grown as of late given the influencer phenomenon. For a legal perspective, *see generally* Alexandra J. Roberts, *False Influencing*, 109 GEO. L. J. 81 (2020).

206. Samuel Arbesman, *The Fraction of Famous People in the World*, WIRED (Jan. 1, 2013), <https://www.wired.com/2013/01/the-fraction-of-famous-people-in-the-world/>.

207. Rosen, *supra* note 17 (“Which is to say, almost no one is famous, so don’t get too down on yourself.”).

208. Marlan, *supra* note 17. Other estimates are lower. 15.7 cases per year, based on computing the averages of the years 2015-2021 (based on 110 right of publicity cases during that period). (C) *Use of Name, Voice or Likeness; Right to Publicity*, k383-k409, WESTLAW, [https://1.next.westlaw.com/Browse/Home/WestKeyNumberSystem?guid=Id0977963a8dc151aca8634aa547dafb5&originationContext=documenttoc&transitionType=Default&contextData=\(sc.Default\)](https://1.next.westlaw.com/Browse/Home/WestKeyNumberSystem?guid=Id0977963a8dc151aca8634aa547dafb5&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)) (last visited on Nov. 15, 2022). By comparison during this time period, there were on average 55.8 trademark cases (383 K1000-1800), 53.5 copyright cases (99 K220-1202), and 93.1 patent cases (291 K401-2094). *West Key Number System*, WESTLAW, [https://1.next.westlaw.com/Browse/Home/WestKeyNumberSystem?transitionType=Default&contextData=\(sc.Default\)](https://1.next.westlaw.com/Browse/Home/WestKeyNumberSystem?transitionType=Default&contextData=(sc.Default)) (last visited on Nov. 15, 2022). The number of right of publicity cases has been trending slowly upwards, though, throughout the decades since the right’s ostensible birth in *Haelan*. Kwall, *supra* note 145, at n.5 (conducting a similar search using Westlaw on Oct. 21, 1997 and noting that “[b]etween 1953 and 1974, there was an average of between four and five right-of-publicity cases decided each year. Between 1975 and 1996, the average was about 14 cases per year.”).

209. Post & Rothman, *supra* note 14, at 130 n.6 (noting that the “uptick in right of publicity filings has been far greater” than the number of published decisions).

210. *Fralely v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011); *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190 (N.D. Cal. 2014); *Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140 (2017); *cf. Hepp v. Facebook, Inc.*, 465 F. Supp. 3d 491 (2020) (suing platform for appropriation of identity by other social media users rather than platform’s own appropriation for purposes of advertising and endorsements, thus potentially triggering § 230 analysis, subject to intellectual property exception); *Cross v. Facebook, Inc.*, 14 Cal. App. 5th 190 (2017) (same). For a helpful overview of social media and its intersection with the right of publicity, see Tune & Levine, *supra* note 25.

States.²¹¹ Over 70 percent of U.S. citizens are social media users.²¹² The non-celebrity aspect of publicity law, which this Article refers to as the pleasurable servitude, by sheer numbers affected deserves far greater recognition in legal and academic discourse.²¹³

The pleasurable servitude may be thought of as part of the “dark matter” of publicity law—that which is constantly occurring but only rarely litigated.²¹⁴ Through broad publicity licenses, the pleasurable servitude strips away the identities of the hundreds of millions of social media users in the United States alone and perhaps billions worldwide.²¹⁵ The phenomenon does not just affect those who are influential and famous but all users who sign up for internet platforms. The pleasurable servitude is also desired (Huxleyan) rather than coerced (Orwellian), as identity-holders willingly (or unwittingly) cede their publicity rights in exchange for use of social media.

As background on the pleasurable servitude, consider that internet platforms like to conduct psychological experiments on their users. A famous example of this is Facebook’s “emotional contagion” study, which occurred in January 2012.²¹⁶ In the experiment, Facebook altered the News Feeds of nearly 700,000 of its users, dividing them into one of two randomly selected groups.²¹⁷ Over the course of one week, one group received content with enhanced positive emotional content and reduced emotional content, and vice versa for

211. STATISTA, *supra* note 20.

212. STATISTA, *supra* note 20.

213. The suggestion is not that the pleasurable servitude is the only non-celebrity right of publicity issue worthy of note. *See, e.g.*, Adam Candeb, *Nakedness and Publicity*, 104 IOWA L. REV. 1747 (2019) (explaining that the right of publicity could provide a cause of action against revenge pornography); Lisa Raimondi, *Biometric Data Regulation and the Right of Publicity: A Path to Regaining Autonomy of Our Commodified Identity*, 16 MASS. L. REV. 198 (2021) (exploring how the right of publicity might be used to address concerns about biometric data ownership rights in situations, such as on social media, where a person’s likeness, as raw data, is essentially bought and sold); Jesse Lempel, *Combating Deepfakes through the Right of Publicity*, LAWFARE (Mar. 30, 2018), <https://www.lawfareblog.com/combating-deepfakes-through-right-publicity> (exploring whether “a victim of a deepfake posted on Facebook or Twitter [could] bring a successful right-of-publicity claim against the platform for misappropriating ‘the commercial use of his or her identity,’” § 230 notwithstanding); Carrie Brown, *Influencing IP: How the Right of Publicity Should Adapt to the Influencer Age*, JIPEL BLOG (Dec. 2020), <https://blog.jipel.law.nyu.edu/2020/12/influencing-ip-how-the-right-of-publicity-should-adapt-to-the-influencer-age/> (exploring the right of publicity’s application to social media influencers).

214. *See* Frye, *supra* note 18.

215. *See infra* notes 260-277 and accompanying discussion.

216. *See* James Grimmelman, *The Facebook Emotional Manipulation Study Sources*, THE LABORATORIUM, BLOG (June 30, 2014, 5:05 PM), http://laboratorium.net/archive/2014/06/30/the_facebook_emotional_manipulation_study_source_.

217. Ralph Schroeder, *Big Data and the brave new world of social media research*, BIG DATA AND SOCIETY 1 (2014).

the other group.²¹⁸ Afterwards, Facebook analyzed the positive and negative words produced by the users on the site to see whether the previous exposure to the positive or negative stimuli impacted the later expressed content.²¹⁹ As anticipated, it certainly did. The experiment showed that the group who was shown more positive words tended to post more positive words, while the group who was shown more negative words tended to post more negative words.²²⁰ Facebook later apologized to an outraged user base.²²¹

The emotional contagion study is probably the most famous experiment to be conducted on social media users. More directly relevant here, though, are Facebook's advertising-based experiments. Advertisers pay social networks to display ads to their billions of users. It is commonly stated that "[w]e are the product; our attention is the product sold to the advertisers."²²² More precisely, according to Jared Lanier, the product is the modification of our behavior.²²³

In September 2006, Facebook created the concept called the "News Feed," a version of which still exists today as a centerpiece of Facebook's platform.²²⁴ Prior to the News Feed, "Facebook was essentially a collection of disconnected user profiles."²²⁵ With the News Feed, Facebook began to broadcast updates of personal details of its users—including relationship status changes—without their knowledge or consent.²²⁶ Many users complained about broadcasting the updates on the News Feeds, and Facebook publicly apologized.²²⁷ A year later, in 2007, Facebook launched a two-part advertising system, called "Social Ads" and "Beacon."

218. *Id.*

219. *Id.*

220. *Id.*

221. Dominic Rushe, *Facebook sorry—almost—for secret psychological experiment on users*, THE GUARDIAN (Oct. 2, 2014), <https://www.theguardian.com/technology/2014/oct/02/facebook-sorry-secret-psychological-experiment-users>.

222. Julien Dimastromatteo, *Social Media are Manipulating your Free Will*, MEDIUM, <https://medium.com/swlh/social-media-are-manipulating-our-free-will-46e4a737e901>.

223. See JARED LANIER, TEN ARGUMENTS FOR DELETING YOUR SOCIAL MEDIA ACCOUNTS RIGHT NOW 10 (2018) ("The core process that allows social media to make money and that also does damage to society is *behavior modification*... techniques that change behavioral patterns in... people.") (emphasis in original).

224. See, e.g., Jillian D'Onfro, *Facebook's News Feed is 10 years old now. This is how the site has changed*, WORLD ECONOMIC FORUM (Sept. 9, 2016), <https://www.weforum.org/agenda/2016/09/facebook-news-feed-is-10-years-old-this-is-how-the-site-has-changed>.

225. *Id.*

226. Natasha Lomas, *A brief history of Facebook's privacy hostility ahead of Zuckerberg's testimony*, TECHCRUNCH (Apr. 10, 2018), <https://techcrunch.com/2018/04/10/a-brief-history-of-facebooks-privacy-hostility-ahead-of-zuckerbergs-testimony/>.

227. Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES (Nov. 30, 2007), <https://www.nytimes.com/2007/11/30/technology/30face.html>

With Social Ads, when users would write something positive about a product or service, Facebook would use their names, images, and reviews in connection with ads on the News Feed. The goal was to entice users to also purchase the products or services by seeing their Friends' endorsements.²²⁸ With Beacon, the concept was similar but directed externally to other commercial websites on the internet. For example, when a Facebook user purchased a product from Amazon or elsewhere, that information would pop up in that user's public profile.²²⁹ Facebook did not adequately inform its users of these advertising mechanisms, and its users were then outraged as they "unwittingly found themselves shilling products on their friends' websites."²³⁰

In 2011, *Cohen v. Facebook, Inc.* was one of the initial class action lawsuits brought against a social network alleging violations of the right of publicity.²³¹ It concerned Facebook's "Friend Finder" service, which generated a list of contacts of people who had not yet signed up for Facebook by searching current users' email accounts.²³² Although this service was not itself necessarily problematic, Facebook also broadcast on the News Feed that the plaintiffs, who were identified by name and profile picture, had tried Friend Finder, in effect serving as endorsements for the service.²³³ The court held that Facebook's terms of service, which, at the time contained broad and ambiguous representations for disclosure of name and profile picture, did not establish consent for this particular use.²³⁴ However, the court dismissed the case for what it viewed as a lack of cognizable injury.²³⁵

Also in 2011, Facebook began running its now infamous "Sponsored Stories" advertisements on the News Feed.²³⁶ Sponsored Stories allowed Facebook to monetize its users' identities—through tracking "likes," "posts," and "check-ins"—and then selling these updates as ads on their friends' News Feeds.²³⁷ Very roughly, Sponsored Stories functioned as follows: (1) users interacted with a company or brand on the site, such as by "liking" their Facebook page; (2) organic News Feed stories were generated regarding those

228. Daniel J. Solove, *Speech, Privacy, and Reputation on the Internet*, in *THE OFFENSIVE INTERNET* 21-22 (2011).

229. *Id.*

230. *Id.* at 21.

231. *See* *Cohen v. Facebook, Inc.*, 798 F. Supp. 2d 1090 (N.D. Cal. 2011).

232. *Id.* at 1091.

233. *Id.*

234. *Id.* at 1097.

235. *Id.*

236. Nathan Ingraham, *Facebook Sponsored Stories will be removed from the site on April 9th*, *THE VERGE* (Jan. 9, 2014, 5:39 PM), <https://www.theverge.com/2014/1/9/5293166/facebook-sponsored-stories-will-be-removed-from-the-site-on-april-9th>.

237. *Id.*

interactions; and (3) advertisers could pay to feature the stories prominently on the News Feeds of users' friends.²³⁸ The endorsement-based ads, viewable in the News Feed, were auto-generated from "actions" taken by users, and featured stories about Pages that users already "Liked."²³⁹ Notably, users were unable to opt-out of seeing Sponsored Stories in the News Feed, or of having their identities used in connection with them.²⁴⁰

According to one description of the value of Sponsored Stories as an advertising mechanism, "[t]he ability to display promoted content alongside organic social content in the popular and highly addictive [N]ews [F]eed is essentially the holy grail for advertisers."²⁴¹ This is because when "users are attentively browsing photos and updates from friends, they'll end up consuming ads as well."²⁴² Indeed, Sponsored Stories are "so similar to organic news feed stories [that] users probably won't notice the difference until they've already internalized an ad's message."²⁴³

Sponsored Stories was the subject of the right of publicity class action lawsuit *Fraley v. Facebook*.²⁴⁴ In *Fraley*, the lead plaintiff in the case, Angel Fraley, had "Liked" the Rosetta Stone company page. This action was then broadcast to her social network on the News Feed.²⁴⁵ In this regard, Fraley represented a class of social media users who alleged right of publicity violations when Facebook did not inform them that their names and images (i.e., profile pictures) would be used to advertise products when they clicked the "Like" button on a brand's Facebook page or engaged in similar activities.²⁴⁶ Notably, Facebook did not allow users to opt-out (i.e., limit or block) of their names and images appearing in connection with Sponsored Stories.²⁴⁷ Nor did Facebook compensate users for their unintended endorsement of the advertised products or services.²⁴⁸

238. Josh Constine, *Facebook Sponsored Story Ads To Appear In The Web News Feed In 2012*, TECHCRUNCH (Dec. 20, 2011), <https://techcrunch.com/2011/12/20/sponsored-stories-news-feed/>.

239. For an illustration of Facebook's Sponsored Stories, see, for example, Laurie Segall, *Facebook's 'sponsored stories' turns your posts into ads*, CNN (Jan. 26, 2011), https://money.cnn.com/2011/01/26/technology/facebook_sponsored_stories/index.htm.

240. Constine, *supra* note 238.

241. Constine, *supra* note 238.

242. Constine, *supra* note 238.

243. Constine, *supra* note 238.

244. *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011).

245. *Id.* at 791.

246. *Id.* at 792.

247. *Id.* at 805.

248. *Id.* at 806.

One of Facebook's main defenses was consent. Facebook claimed that by agreeing to its terms of service, users provided the social network with permission to use their names and pictures in connection with commercial, sponsored, or related content.²⁴⁹ Yet, plaintiffs had all registered for Facebook prior to the rollout of Sponsored Stories and were not asked to consent again to a modified terms of service before the launch of the program.²⁵⁰ Plaintiffs thus alleged that they did not know that their use of the "Like" button would be "interpreted and publicized by Facebook as an endorsement of those advertisers, products, services, or brands."²⁵¹

The plaintiffs in *Fralely* encountered difficulties in their right of publicity claim partly because they had assigned their publicity rights to Facebook for advertising and endorsement purposes per the terms of service.²⁵² According to the California District Court in *Fralely*, plaintiffs "faced a substantial hurdle in proving a lack of consent, either express or implied. While those issues could not be decided in Facebook's favor at the pleading stage, there was a significant risk that, if the litigation was to proceed to trial, plaintiffs would be found to have consented."²⁵³ Ultimately, the lawsuit settled for a modest \$10 per claimant.²⁵⁴

In 2014, another right of publicity class action, *Perkins v. LinkedIn*, involved a challenge to professional networking platform LinkedIn's use of a service called "Add Connections."²⁵⁵ Add Connections allowed LinkedIn users to import contacts from their email accounts and then email connection invites to their contacts, inviting them to connect on LinkedIn, using plaintiffs' names and likenesses in the endorsement emails. For example, an email recipient may receive an email from LinkedIn stating, "I'd like to add you to my professional network—Paul Perkins."²⁵⁶ Then, on receiving a member's authorization, LinkedIn would send an email to the member's email contacts who were not already members of LinkedIn. If that connection invite was not accepted within a certain amount of time, up to two further emails were sent reminding

249. *Id.* at 805–06.

250. *Id.*

251. *Id.* at 792.

252. Another major issue was that, as private figures, their personas had little financial value for assessing injury. For an analysis of this issue specifically, see Marlan, *supra* note 15, at 468–70.

253. *Fralely v. Facebook, Inc.*, 966 F. Supp. 2d. 939, 942 (N.D. Cal. 2013).

254. Settlement Notice [*Fralely v. Facebook*], SANTA CLARA L. DIGIT. COMMONS (Jan. 2, 2013) <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1272&context=historical>.

255. *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1222, 1225 (N.D. Cal. 2014).

256. *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1200 (N.D. Cal. 2014).

the recipient that the connection invite was pending.²⁵⁷ Ultimately, the class action settled for \$13 million.²⁵⁸

In response to lawsuits such as *Coben*, *Fralely*, and *Perkins*, internet platforms have enacted (or tightened) the “pleasurable servitude”—the mandatory license of social media users’ rights of publicity in exchange for use of the service. Importantly, consent functions as a complete defense to right of publicity claims. Thus, conduct that would otherwise infringe the right of publicity is not actionable if the holder of the right consents to the use.²⁵⁹ However, a user who has not consented or consented only to a limited use of their identity may still prevail on a right of publicity claim that is outside the scope of the terms.²⁶⁰ Social networks must thus be strategic in crafting their terms of service to obtain the express consent of their users’ identities for commercial purposes. For example, Facebook’s terms of service now reads, in the relevant part:

Permission to use your name, profile picture, and information about your actions with ads and sponsored content: You give us permission to use your name and profile picture and information about actions you have taken on Facebook next to or in connection with ads, offers, and other sponsored content that we display across our Products, without any compensation to you. For example, we may show your friends that you are interested in an advertised event or have liked a Page created by a brand that has paid us to display its ads on Facebook.²⁶¹

The pleasurable servitude is an example of what Margaret Jane Radin describes as the “unwitting contract.” Most websites have a terms of service, which most users do not actually read. When a user does click on it, “pages of boilerplate open out, telling the user that she is bound to these terms, that she has ‘agreed’ to them simply by the act of looking at the site, and, moreover, that the owner may change the terms from time to time and that the user will be bound by the new terms as well.”²⁶² This type of contract is called

257. *Id.*

258. *See, e.g.*, Eric Goldman, *The Perkins v. LinkedIn Class Action Was Badly Bungled*, FORBES (Oct. 3, 2015, 10:38 AM), <https://www.forbes.com/sites/ericgoldman/2015/10/03/the-perkins-v-linkedin-class-actionsettlement-notification-was-badly-bungled/#5190d7844e0c>.

259. Tune & Levine, *supra* note 25, at 16.

260. Tune & Levine, *supra* note 25, at 17.

261. Facebook, *Terms of Service*, <https://www.facebook.com/terms.php> (last visited July 24, 2021).

262. MARGARET JANE RADIN, *BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 12* (2012).

“browsewrap.”²⁶³ Where users affirmatively declare acceptance by clicking “I agree,” the agreement is instead referred to as a “clickwrap” agreement. Generally, courts enforce clickwrap agreements, so social networks are incentivized to use clickwrap. In contrast, browsewrap agreements are often, but not always, declared unenforceable.²⁶⁴

Through browsewrap or clickwrap contracts, social media users’ publicity rights are constantly being transferred to social networks. This specious form of consent occurs either willingly (because users realize they have no other option) or unwittingly (because they are too distracted or disinterested to read the terms of service). For instance, Instagram, owned by Meta Platforms, Inc. (formerly Facebook, Inc.), contains a substantially similar clause to Facebook’s above clause.²⁶⁵ The multimedia messaging app Snapchat’s terms of service demands an even broader right of publicity license in exchange for use of the platform:

When you appear in, create, upload, post, or send Public Content (including your Bitmoji), you also grant Snap, our affiliates, other users of the Services, and our business partners an unrestricted, worldwide, royalty-free, irrevocable, and perpetual right and license to use the name, likeness, and voice, of anyone featured in your Public Content for commercial and non-commercial purposes. This means, among other things, that you will not be entitled to any compensation if your content, videos, photos, sound recordings, musical compositions, name, likeness, or voice are used by us, our affiliates, users of the Services, or our business partners.²⁶⁶

Other platforms have similar pleasurable servitudes. LinkedIn’s terms of service state that “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.”²⁶⁷ YouTube frames the issue as a “right to monetize”—“You grant to YouTube the right to monetize your Content on the Service (and such monetization may include displaying ads on or within Content or charging users a fee for access). This

263. *Id.*

264. *Id.*

265. Instagram, *Terms of Use*, (2021) (last visited Aug. 2, 2021), <https://help.instagram.com/581066165581870>.

266. *Supra* note 28. *Terms of Service*, SNAP INC., (2021) (last visited Nov. 2, 2022), <https://snap.com/en-US/terms>.

267. *User Agreement*, LINKEDIN, <https://www.linkedin.com/legal/user-agreement> (last visited Aug. 2, 2021).

Agreement does not entitle you to any payments.”²⁶⁸ TikTok’s terms of service state:

By posting User Content to or through the Services, you waive any rights to prior inspection or approval of any marketing or promotional materials related to such User Content. You also waive any and all rights of privacy, publicity, or any other rights of a similar nature in connection with your User Content, or any portion thereof.²⁶⁹

Here, rather than licensing their users’ rights of publicity, as do Facebook and Snapchat, TikTok includes a broad publicity (and privacy) waiver, accomplishing much the same consent scheme, assuming courts would hold such a waiver valid.²⁷⁰ As Radin argues persuasively, courts should not enforce such waiver provisions, because valid consent is a major requirement for an enforceable contract.²⁷¹ Rather than valid consent, terms of service like the ones discussed above are adhesion contracts based often on “sheer ignorance.”²⁷²

The pleasurable servitude is not limited to the major social networks. For instance, in the 2019 case of *Dancel v. Groupon*, a class of plaintiffs alleged that Groupon, Inc. violated the Illinois Right of Publicity Act (IRPA) by harvesting plaintiffs’ photos and usernames from Instagram, and then using them to advertise vouchers for Illinois businesses on the Groupon platform without consent.²⁷³ To use Instagram, as is typical with other social networks, individuals must create a username, and can then begin posting photos on the platform. The photos can then be viewed by others who visit the platform. Instagram users can also “tag” their photos with information, such as the location where a given photo was taken and the usernames of others who appear in the photo.²⁷⁴

268. *Terms of Service*, YOUTUBE, <https://www.youtube.com/static?template=terms> (last visited Aug. 2, 2021).

269. *Terms of Service*, TIKTOK, <https://www.tiktok.com/legal/terms-of-service?lang=en> (last visited Aug. 2, 2021).

270. See Anthony M. Ramirez & Katherine DeVries, *Just Browsing: District Court Finds Browsewrap Agreement Enforceable*, SOCIALLY AWARE BLOG (Nov. 14, 2019), <https://www.sociallyawareblog.com/2019/11/04/just-browsing-district-court-finds-browsewrap-agreement-enforceable/>.

271. Radin, *supra* note 23, at 19.

272. Radin, *supra* note 23, at 21.

273. *Dancel v. Groupon, Inc.*, 949 F.3d 999, 1002 (2019).

274. See *Tagging and Mentions*, INSTAGRAM, <https://help.instagram.com/627963287377328> (last visited Nov. 8, 2022) (providing instructions on how to tag photos on Instagram).

Groupon is a platform that sells discount vouchers for goods and services at local businesses, often restaurants. Here, Groupon, in “scraping” Instagram accounts, found a photo that plaintiff Christine Dancel had posted on Instagram that depicted a restaurant in Mt. Vernon, Illinois.²⁷⁵ Without Dancel’s knowledge, Groupon used her photo and username (“meowchristine”) in connection with selling vouchers to that restaurant.²⁷⁶ Groupon also did this to other Instagram users on a mass scale, harvesting usernames and photos to advertise its vouchers for other businesses.²⁷⁷ Ultimately, the lawsuit was dismissed, because the Seventh Circuit held that Instagram usernames do not constitute an aspect of identity common to the entire class. Groupon’s terms of service now reads:

You grant Groupon a royalty-free, perpetual, irrevocable, sublicensable, fully paid-up, non-exclusive, transferrable, worldwide license and right to use, commercial use, display and distribute any Personal Information in connection with your User Content in accordance with these Terms of Use, including, without limitation, a right to offer for sale and to sell such rights in Personal Information, whether the User Content appears alone or as part of other works, and in any form, media or technology, whether now known or hereinafter developed, and to sublicense such rights through multiple tiers of sublicensees, all without compensation to you.²⁷⁸

Terms of service agreement consent provisions, such as the examples above, constitute exculpatory provisions for the use of user identities for advertising and endorsement purposes. Thus, by demanding broad publicity licenses or waivers, as it stands now, internet platforms have likely drafted their way out of liability for appropriation of their users’ publicity rights. Again, if a user does not consent to the applicable terms of service (and privacy policy), they cannot use the social network. In effect, by consenting to terms of service on social media, ordinary citizens license rights in their identities to internet platforms in exchange for access to the pleasures and comforts of digital worlds. Through the pleasurable servitude, internet platforms become the publicity rights holders of the identities of their hundreds of millions of users in the United States. The pleasurable servitude thus results in widespread identity alienation and identity commodification, which can be viewed as harmful when seen through the lens of a Huxleyan dystopia.

275. *Dancel*, 949 F.3d at 1002.

276. *Dancel*, 949 F.3d at 1002.

277. *See Dancel*, 949 F.3d at 1002.

278. Groupon, Inc., *Terms of Use*, (2019) (last visited Aug. 2, 2021), <https://www.groupon.com/legal/termservice>.

IV. PUBLICITY'S BRAVE NEW WORLD

*We are not our own any more than what we possess is our own.*²⁷⁹

This Part proposes a regulatory path forward for the right of publicity in responding to the online publicity licensing phenomenon. This Part first discusses the pleasurable servitude as a matter of social and economic injustice—an instance of online manipulation and emblematic of surveillance capitalism.²⁸⁰ It next proposes regulation in the form of “publicity policies”—analogous to privacy policies—with the goal of increasing awareness among users of social networks and other internet websites regarding identity appropriation. Through publicity policies, social media users could customize their publicity settings through an opt-out regime. This Part lastly discusses the First Amendment balance in the context of the pleasurable servitude. To the extent that social networks claim a free speech defense in cases like *Fraley* and *Perkins*, or to evade regulation of the issue more broadly, the defense should be denied as commercial speech outside the scope of core First Amendment protection.

A. MANIPULATIVE PUBLICITY

Locating the relationship between internet platforms and their users within a Huxleyan dystopia highlights the harms to users’ publicity rights in ways that appropriately characterizes the manipulative dynamics of that relationship. In particular, the pleasurable servitude involves aspects of (1) online manipulation, (2) dark patterns, and (3) surveillance capitalism. These three subjects will be discussed in turn.

Susser, Roesler, and Nissenbaum define online manipulation as “the ability of data collectors to use information about individuals to manipulate them.”²⁸¹ Such manipulation “disrupts our capacity for self-authorship—it presumes to decide for us how and why we ought to live.”²⁸² In considering that identities are transferred online, through targeted advertisements, as a form of data, the pleasurable servitude can be seen as an aspect of online manipulation.²⁸³ And the targeted advertisements and endorsements that are “consented to” through these terms of service have long been a quintessential form of online manipulation discussed among privacy scholars.

279. HUXLEY, *supra* note 8, at 278.

280. See Zuboff, *supra* note 27.

281. Susser, et al., *supra* note 26, at 1.

282. Susser, et al., *supra* note 26, at 4.

283. See Spencer, *supra* note 26, at 980 (noting that “marketers have already proven with online behavioral advertising that they can target different advertisements, offers, and terms of service in real time.”).

Along these lines, the pleasurable servitude is characteristic of what Ryan Calo refers to as “digital market manipulation,” or “nudging for profit.”²⁸⁴ Digital market manipulation refers to the ability of advertisers to collect data about consumers and then use that data to personalize their users’ experience by taking advantage of their cognitive limitations.²⁸⁵ This involves “uncover[ing] and trigger[ing] consumer frailty at an individual level” in an attempt to “set prices, draft contracts, minimize perceptions of danger or risk, and otherwise attempt to extract as much rent as possible from consumers.”²⁸⁶ Here, publicity appropriation—enabling consent for targeted, endorsement-based advertising—is a form of means-based targeting. In essence, this means “matching the right advertising *pitch* with the right person, based on the premise that people vary in their susceptibility to various forms of persuasion.”²⁸⁷

The pleasurable servitude may similarly be thought of as a “dark pattern”—a design that functions to trick users into doing what they ordinarily would not do, such as handing over their personal data, in this case transferring their publicity rights through online terms of service.²⁸⁸ According to Senator Mark R. Warner (D-VA), former technology executive and Chairman of the Senate Select Committee on Intelligence: “For years, social media platforms have been relying on all sorts of tricks and tools to convince users to hand over their personal data without really understanding what they are consenting to.”²⁸⁹ Warner notes that one of the most manipulative strategies is reliance on dark patterns—“deceptive interfaces and default settings, drawing on tricks of behavior psychology, designed to undermine user autonomy and push consumers into doing things they wouldn’t otherwise do, like hand over all of their personal data to be exploited for commercial purposes.”²⁹⁰

More broadly, the pleasurable servitude is a form of “behavior modification” emblematic of what Shoshana Zuboff labels “surveillance capitalism”—“declaring private human experience as free raw material for

284. Calo, *supra* note 26, at 1001.

285. See Calo, *supra* note 26, at 999.

286. Calo, *supra* note 26, at 995, 1001.

287. Renee Boucher Ferguson, *Is Digital Advertising a New Form of Market Manipulation?*, MIT SLOAN MGMT. REV. (Sept. 24, 2013), <https://sloanreview.mit.edu/article/is-digital-advertising-a-new-form-of-market-manipulation/>.

288. Arunesh Mathur, Jonathan Mayur & Mihir Kshirsagar, *What Makes a Dark Pattern . . . Dark?*, CHI '21: PROCEEDINGS OF THE 2021 CHI CONFERENCE ON HUM. FACTORS IN COMPUT. SYS. 3 (2021).

289. Mark R. Warner, U.S. Senator from the Commonwealth of Virginia, Press Release (Apr. 9, 2019), <https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns>.

290. *Id.*

translation into production and sales. Once private human experience is claimed for the market, it is translated into behavioral data for computational production.²⁹¹ Here, the claimed private human experience is user identity—name, image, or likeness.

This manipulation through terms of service and its resulting enablement of targeted advertising experiments is Huxleyan, differing from an Orwellian world of top-down surveillance. The social network experiments involve playing with their users' minds in such a way that they accept, or even delight in it.²⁹² A form of social conditioning, the purported goal of manipulating social media users is to improve the user experience (i.e., pleasure) on the platforms.²⁹³ Of course, improving experience is synonymous with selling targeted advertisements and thus increasing revenue. Such aims are also consistent with the conspicuous consumption depicted in *Brave New World*.²⁹⁴

The pleasurable servitude results in social and economic injustice. Some would argue that social networks are delivering a valuable service to users and therefore should be able to appropriate publicity rights for purposes of identity-based advertising, sponsorship, and endorsements when and how they want.²⁹⁵ Consider, though, that it is increasingly difficult to live an internet and social media free life. Indeed, new technologies are “a pervasive and insistent part of everyday life” and “it is becoming increasingly hard to forgo using these technologies, especially when they are very useful and beneficial.”²⁹⁶ And “individuals are compelled to engage with social media to maintain their “social circles, professional presence, or romantic relationships.”²⁹⁷

291. SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM* 270 (2019) (explaining that through technological behavior modification, we “sacrifice our right to the future tense, which comprises our will to will, our autonomy, our decision rights, our privacy, and, indeed, our human rights”).

292. Ralph Schroeder, *Big Data and the Brave New World of social media research*, *BIG DATA AND SOCIETY* 3-4 (2014) (explaining “that it is more relevant to invoke Huxley’s *Brave New World* [than 1984], where companies and governments are able to play with people’s minds, and do so in a way such that users, knowingly or unknowingly (and it may not be easy to tell the difference), come to accept and embrace this”).

293. *Id.* at 4.

294. *See id.* (“[I]mproving experience and services could also just mean selling more products, or manipulating people’s political behavior.”).

295. *See* Garrie, *supra* note 30 (discussing the mutual convenience of the technological relationship to both the social networks and its users).

296. Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 *Geo. Wash. L. Rev.* 1, 37 (2021) [hereinafter Solove, *Myth of Privacy Paradox*]; *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (noting that “cell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society”).

297. Raimondi, *supra* note 213, at 200.

Therefore, forgoing use of internet platforms might mean, particularly in a pandemic era, living “an isolated and hermetic existence.”²⁹⁸ Moreover, social media is designed to be as addictive as possible. Many simply do not have the will to resist it.²⁹⁹ As former president of Facebook Sean Parker confessed, the site is designed to exploit our “vulnerability” and to “consume as much of [our time and conscious attention as possible].”³⁰⁰

For those who use social media, the licensing of one’s identity and for commodification by the platforms is done willingly (or at least without obvious coercion). But such consent is also a mandatory condition to use the platforms. As the Huxleyan metaphor demonstrates, the fact that individuals *voluntarily* trade their publicity for use of platforms does not demonstrate that such contractual transactions are valuable or conscionable.³⁰¹ Rather, the licensing of publicity rights is normatively undesirable based on (1) individual autonomy and dignity-related concerns, as well as (2) broader social and political reasons. Given such normative and democratic concerns elaborated below, courts should hold pleasurable servitude contracts—whether clickwrap or browsewrap—unenforceable. Moreover, as will be discussed in Part IV.B, this is an area that should be the subject of legislative action.

298. Solove, *Myth of Privacy Paradox*, *supra* note 296, at 30.

299. See Yubo Hou, *Social media addiction: Its impact, mediation, and intervention*, 13 CYBERPSYCHOLOGY: J. PSYCHOSOCIAL RSCH. ON CYBERSPACE 1, 1 (2019) (“Individuals with social media addiction are often overly concerned about social media and are driven by an uncontrollable urge to log on and use social media.”); Stephanie Plamondon Baer, *Innovations Hidden Externalities*, 47 BYU L. REV. 1385, 1411 (2022) (“Interactions with media innovations, like the texting and social networking applications found on smartphones, provide emotional gratification.”); see also Shiri Melumed and Michel Tuan Pham, *The Smartphone as a Pacifying Technology*, 47 J. CONSUMER RSCH. 237 (2019) (explaining that the smartphone itself, beyond its applications like social media, is an addictive technology). The addictive and exploitive nature of social media was popularized in Tristan Harris’s documentary *The Social Dilemma*, NETFLIX (2020).

300. Olivia Solon, *Ex-Facebook president Sean Parker: site made to exploit human ‘vulnerability*, THE GUARDIAN (Nov. 9, 2017), <https://www.theguardian.com/technology/2017/nov/09/facebook-sean-parker-vulnerability-brain-psychology>. More recently, Facebook whistleblower Frances Haugen revealed that Facebook “failed to address negative effects of its social media products,” realizing “that if they change the algorithm to be safer, people will spend less time on the site, they’ll click on less ads, they’ll make less money.” Chad De Guzman, *The Facebook Whistleblower Revealed Herself on 60 Minutes. Here’s What You Need to Know*, TIME (Oct. 4, 2021) <https://time.com/6103645/facebook-whistleblower-frances-haugen/>.

301. See Solove, *Myth of Privacy Paradox*, *supra* note 296, at 29 (“The fact that people trade their privacy for products or services does not mean that these transactions are desirable in their current form.”).

1. *Autonomy and Dignity Concerns*

The pleasurable servitude threatens autonomy and dignity in much the same way as data privacy breaches do.³⁰² The concept of autonomy is essential to a liberal democratic society.³⁰³ Autonomy refers to an individual's capacity to make "meaningfully independent decisions."³⁰⁴ Online manipulation threatens the autonomy of social media users by leading them to act in ways they have not chosen and for inauthentic reasons.³⁰⁵

The problem is particularly glaring in the right of publicity context given that "human identity is a self-evident property right."³⁰⁶ Identity is an aspect of personhood.³⁰⁷ The distinction, though, is that although personhood carries an "intrinsic worth" belonging equally to all human beings, identities are not shared equally but rather constitute the aspects of the self that are unique from others.³⁰⁸ As such, the forced commodification of identity on social media can be seen as an assault on dignity that denies "the conditions of individuation necessary to the proper respect for and development of one's personhood."³⁰⁹ It does this by "treating people as experimental subjects and mere means to an end."³¹⁰

From a reputational standpoint too, individuals should be respected in how they want to be portrayed, such as having the ability to opt-out of having their identities used in connection with targeted advertisements or otherwise commodified. Although complete control of our reputations is not a reality, either in the physical or digital world, citizens should have some ability to protect their reputations from unfair harm on the internet and social media.³¹¹

As an example of autonomy, dignity, and reputational harm, consider the 2016 right of publicity class action lawsuit *Parker v. Hey, Inc.*, where Twitter users' profiles were turned into trading cards without their consent.³¹² *Parker* involved an App called "Stolen," which allowed players to collect the Twitter

302. For literature on the connection between privacy breaches and autonomy, see generally Susser et al., *supra* note 26; Luciano Floridi, *On Human Dignity: a Foundation for the Right to Privacy*, 29 *Philosophy & Technology* 307-312 (2016);

303. Susser et al., *supra* note 26, at 8.

304. Susser et al., *supra* note 26, at 8.

305. Susser et al., *supra* note 26, at 8.

306. Daniel Gervais & Martin L. Holmes, *Fame, Property & Identity: The Purpose and Scope of the Right of Publicity*, 25 *FORDHAM INTELL. PROP. MEDIA & ENT. L.J.* 181, 194 (2014).

307. Kahn, *supra* note 5, at 218.

308. Kahn, *supra* note 5, at 218.

309. Kahn, *supra* note 5, at 219.

310. Spencer, *supra* note 5, at 991.

311. Solove, *Myth of Privacy Paradox*, *supra* note 296, at 38.

312. *Parker v. Hey, Inc.*, Case No. CGC-17-556257, 2017 Cal. Super LEXIS 609, *1-2 (Super. Ct. Cal. Apr. 14, 2017).

profiles of real-life people as if they were baseball cards.³¹³ Although not created by Twitter, the App was endorsed by Twitter, at least initially, and relied exclusively on data from Twitter. Hey, Inc., the App’s maker, accessed the data by partnering with Twitter, an arrangement that allowed it to access the Twitter API through which Twitter disclosed individuals’ names and images.³¹⁴

According to journalist Lauren Hockenson’s description of Stolen’s features, the game “essentially sucks in all of the available public data from Twitter and assigns value to user names.”³¹⁵ Players are then “encouraged to buy these users with currency You buy people, and then other people pay more than you to take that person away.”³¹⁶ For Hockenson, “it felt particularly weird going on an app I only knew about a few days ago to find people who follow me on Twitter have driven up my value. That people are sparring back and forth to take ownership of my account.”³¹⁷

Hockenson notes that the App “commoditize[s] users without their knowledge” and, in doing so, “crafts a potential opening for harassment” considering people who “own” others’ profiles can rename them.³¹⁸ As such, [i]t’s not too much of a mental stretch to see how this can be used to harm someone personally,” given that “you can’t opt out of the game.”³¹⁹

2. *Political and Democratic Concerns*

In addition to being problematic from the perspective of individual autonomy, mass identity transfer furthers technology companies’ monopoly on collective human capital.³²⁰ In this sense, the pleasurable servitude can be seen as a collective harm from a broader social, political, and democratic perspective. As New York Attorney General Letitia James puts it, “[n]o

313. *Id.* As such, the facts evoke an eerie consent-free subversion of Judge Frank’s *Haelan* opinion. See *Haelan Lab’ys, Inc. v. Topps Chewing Gum, Inc.*, 202 F.2d 866, 867 (2d Cir. 1953) and accompanying discussion.

314. *Parker*, 2017 Cal. Super LEXIS 609, at *2-3.

315. Lauren Hockenson, *Here’s the 411 on Stolen—the app that turns your Twitter account into a commodity*, THE NEXT WEB (Jan. 13, 2016), <https://thenextweb.com/news/what-the-hell-is-stolen>.

316. *Id.*

317. *Id.*

318. *Id.*

319. *Id.*

320. See, e.g., RADIN, *supra* note 23, at 35 (“Widespread boilerplate undermines the rationale that justifies the state’s power to organize the polity; and it converts rights enacted and guaranteed by the state into rights that can be ‘condemned’ by private firms.”). Marks, *supra* note 81, at 589 (“By deploying dark patterns and other coercive design features, tech companies . . . [gain] monopolistic power over human behavior, which threatens democracy and human autonomy.”).

company should have this much unchecked power over our personal information and our social interactions.”³²¹ And as Radin argues in *Boilerplate*, contracts of adhesion such as terms of service displaces legal regimes created by the state with governance regimes more favorable to corporations—in effect “transporting recipients to a firm’s own preferred legal universe” and thus causing “democratic degradation” that undermines public ordering.³²²

Along these lines, Michel Foucault labeled the ability to manipulate human capital “biopower”—literally, having power over bodies, or “an explosion of numerous and diverse techniques for achieving the subjugation of bodies and the control of populations.”³²³ In distinguishing biopower from an Orwellian subjugation, Foucault used the term to describe “a power bent on generating forces making them grow, and ordering them, rather than one dedicated to impeding them, making them submit, or destroying them.”³²⁴ Like the Huxleyan warning of a utilitarian society gone awry, Foucault envisions modern humans as “an animal whose politics places his existence as a living being in question.”³²⁵ Both “the disciplinary power mechanisms of the body and the regulatory mechanisms of the population, constitute the modern incarnation of power relations, labeled as *biopower*.”³²⁶

In preventing what Mason Marks labels “biosupremacy” by internet platforms—a monopoly on biopower—reasonable limits on the transferability of identity-based rights—name, image, likeness—could serve as a limit on the immense power that internet platforms currently possess over their users.³²⁷ In the pleasurable servitude cases, identity is transferred as a form of data. As Daniel Solove puts it, “[p]ersonal data can be used to affect our reputations; and it can be used to influence our decisions and shape our behavior. And it

321. *N.Y. Attorney General Asks Courts to Take Action Against Facebook*, N.Y. TIMES (Dec. 9, 2020), <https://www.nytimes.com/video/us/politics/10000007495190/new-york-attorney-general-facebook-antitrust.html>.

322. See RADIN, *supra* note 23, at 35 (“[Boilerplate] threatens the distinction between public and private ordering, and indeed the ideal of private ordering itself. In addition to undermining or bypassing the system of rights structures enacted and guaranteed by the state, the degradation of our commitment to democratic political ordering includes several other interlocked deficiencies.”).

323. MICHEL FOUCAULT, *HISTORY OF SEXUALITY (THE WILL TO KNOWLEDGE: HISTORY OF SEXUALITY)* Vol. 1, 140 (1976).

324. *Id.* at 136.

325. *Id.* at 146.

326. Vernon W. Cisney and Nicolae Morar, *Why Biopower? Why Now?*, 5 in *BIOPOWER: FOUCAULT AND BEYOND* (2015).

327. See Marks, *supra* note 81, at 519 (“When firms acquire a dominant share of biopower, influencing enough traits in sufficiently large populations, they achieve *biosupremacy* . . . monopolistic power over human behavior.”).

can be used as a tool to exercise control over us.”³²⁸ In other words, if we have no control over our data (no less our very identity)—how it is being used, and what it is being used for—we remain at the mercy of large technology companies and their market power.

For instance, currently, online publicity licenses are non-exclusive.³²⁹ But if the terms of service were to change to claim exclusive publicity license in users’ identities, internet platforms may singularly possess property rights in them.³³⁰ In such a dystopian vision, to use social networks, one would have to agree to an exclusive, perpetual license to their name, image, or likeness. In essence, the individual will have signed away their right of publicity.³³¹ The internet platform could then impose limits on its users’ ability to market themselves or use their likenesses in future advertisements without their consent. As scholars have previously noted, such a licensing regime would be profoundly undemocratic and freedom limiting.³³²

Would internet platforms venture to take such an exclusive right in user identities, or would they be constrained by ethics or by market principles? The answer is not totally clear, and it may be pessimistic to predict that a technology corporation would claim exclusivity in the legal identity of its millions or billions of users. Yet, short of citizen activism or legal regulation, the power is in the hands of social networks. As one commentator remarked regarding Facebook CEO Mark Zuckerberg: “There is nothing that constrains what [Zuckerberg] can do ... This is a level of concentrated power in the hands of one person that I’m not sure we’ve ever seen anywhere in history. And whatever his intentions are, whatever kind of person he is, we should never have allowed this to happen.”³³³

B. PUBLICITY POLICIES

To the extent that the right of publicity remains a transferable, commercial right, individuals should be educated in this regard. As a mechanism for doing so, this section analogizes to privacy policies. For example, California’s privacy law requires “operators of commercial web sites or online services that collect

328. Daniel Solove, *10 Reasons Why Privacy Matters*, TEACH PRIVACY (Jan. 20, 2014), <https://teachprivacy.com/10-reasons-privacy-matters/>.

329. See ROTHMAN, RIGHT OF PUBLICITY, *supra* note 15, at 128.

330. See ROTHMAN, RIGHT OF PUBLICITY, *supra* note 15, at 128.

331. Solove, *Consent Dilemma*, *supra* note 23, at 1880 (“Consent legitimizes nearly any form of collection, use, or disclosure of personal data.”).

332. ROTHMAN, RIGHT OF PUBLICITY, *supra* note 15, at 128; Raimondi, *supra* note 213, at 216.

333. NYU Law School, *Monopolization and Abuse: Application to Platforms and Digital Markets*, YOUTUBE, (May 12, 2020), <https://www.youtube.com/watch?v=XSSGaQ9xwd8>.

personal information on California residents through a website to conspicuously post a privacy policy on the site and to comply with its policy.”³³⁴ Those who fail to do so risk civil litigation under unfair competition laws.³³⁵

For example, New York passed a comprehensive right of publicity law that became effective on May 29, 2021. The law created a transferable and descendible right of publicity, and also touched upon the online publicity phenomenon by making illegal sexually explicit deepfakes and protecting digital avatars and digital voices as aspects of the commercial identity.³³⁶ But it did not address the pleasurable servitude.³³⁷ Ideally, the law would have regulated social networks so that they are not able to claim the publicity rights of users for purposes of advertising, sponsorships, and endorsements.³³⁸ At least though, it should have included a provision requiring “publicity policies” to promote awareness among social media users of the mass transfer of publicity rights required to use the services, and subsequent commodification of their identities.

The inclusion of publicity policies could function as a sort of media literacy regarding the right of publicity. In invoking Marshall McLuhan’s philosophy of media ecology, Strate explains that our technology and media function as “environments” which can “fad[e] into the background as they become routine, thereby becoming invisible to us.”³³⁹ Along these lines, Postman remarked that “technopoly eliminates alternatives to itself precisely the way Aldous Huxley outlined in *Brave New World*. It does not make them illegal. It

334. *Cal. Bus. & Prof. Code* §§ 22575-22579; California Online Privacy Protection Act (CalOPPA) (2013), <https://consumercial.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/>

335. *Id.*

336. For a sampling of the literature on the deep fake issue, see generally Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019); Matthew B. Kugler and Carly Pace, *Deepfake Privacy: Attitudes and Regulations*, 116 NW. U. L. REV. 611 (2021); Douglas Harris, *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, 17 DUKE L. & TECH. REV. 99 (2019); Rebecca A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn’s Next Tragic Act*, 88 FORDHAM L. REV. 887 (2019); Anne Pechenik Gieseke, “*The New Weapon of Choice*”: *Law’s Current Inability to Properly Address Deepfake Pornography*, 73 VAND. L. REV. 1479 (2020).

337. See Judith Bass, *New York’s New Right of Publicity Law: Protecting Performers and Producers*, NEW YORK STATE BAR ASSOCIATION (Mar. 17, 2021), <https://nysba.org/new-yorks-new-right-of-publicity-law-protecting-performers-and-producers>.

338. I discuss this point further in a previous work. See Marlan, *supra* note 15, at 463.

339. Strate, *supra* note 192, at 143 (citing MARSHAL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN (1964)).

does not make them immoral. It does not even make them unpopular. It makes them invisible and therefore irrelevant.”³⁴⁰

To counteract such technological fatalism, Postman suggested that education should serve a cybernetic function. To this end, “education [should be] based on literacy and typography, on the spoken and written word, and on reason and rationality, against the extremes of idolatry and efficiency, image culture and technopoly.”³⁴¹ Postman writes regarding the importance of media literacy: “[Aldous Huxley] believed . . . that we are in a race between education and disaster, and he wrote continuously about the necessity of our understanding the politics and epistemology of media.”³⁴² Indeed, “what afflicted the people in *Brave New World* was not that they were laughing instead of thinking, but that they did not know what they were laughing about and why they had stopped thinking.”³⁴³

In applying media literacy to publicity law, privacy policies educate the public about the contractual relationship between users and social media platforms. Among other disclosures, privacy policies typically define the extent to which social media platforms or other websites can use user data to generate revenue through targeted advertising. Prior to regulatory intervention, privacy policies were often embedded within a website’s terms of service. However, several laws now require distinctive and easily found privacy policies. For example, under California’s privacy law:

The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information. The privacy policy must also provide information on the operator’s online tracking practices. An operator is in violation for failure to post a policy within 30 days of being notified of noncompliance, or if the operator either knowingly and willfully or negligently and materially fails to comply with the provisions of its policy.³⁴⁴

Analogously, legislation mandating publicity policies could serve an important disclosure function as to the appropriation of social media users’ commercial identities (e.g., name, image, and likeness) across social media and

340. NEIL POSTMAN, *TECHNOPOLY: THE SURRENDER OF CULTURE TO TECHNOLOGY* 71-2 (1992) (defining a “technopoly” as a society in which technology is deified; where “the culture seeks its authorization in technology, finds its satisfactions in technology, and takes its orders from technology”).

341. Strate, *supra* note 192, at 143.

342. POSTMAN, *supra* note 1, at 163.

343. POSTMAN, *supra* note 1, at 163.

344. CalOPPA, *Cal. Bus. & Prof. Code* § 22575.

on the internet. Like California's privacy policy regulations, social media platforms should not be allowed to bury publicity-related disclosures in the terms of service. Instead, they should be made to conspicuously post a publicity policy on their sites and comply with it. The publicity policy should identify the aspects of the identity—name, image, or likeness—that the platform will collect, and to what ends the platform will use the information. Having social media users consent by way of clickthrough publicity policies would be a heightened form of consent, at least as compared to provisions within the browsewrap terms of service.

Inherent within the publicity policy should also be users' ability to opt-out of platforms' use of identity in connection with commercial and sponsored conduct.³⁴⁵ Users should be able to customize their settings regarding the scope of their publicity license, as well as permissions regarding the types of identity-based endorsements and sponsorships their publicity rights will be used in connection with. An opt-out regime granted through a publicity policy, while not ideal, is a sensible, middle of the road approach to consent. It would shift some of the power and control back to social media users while still allowing platforms the economic power to fuel their platform through (targeted) advertisements. This sort of publicity "self-management" will not alone solve the issue.³⁴⁶ But legislation mandating the use by internet platforms of publicity policies would be a realistic start to regulating the area in drawing attention to the issue on a macro level.

Some will object to the publicity policy proposal based on the failure of analogous privacy policies—"privacy self-management" or user "control"—as an all-encompassing solution to privacy concerns. As Woodrow Hartzog argues, "the focus on control distracts you from what really affects your privacy in the modern age . . . It is all in the design."³⁴⁷ But this control-oriented proposal is not meant as a complete solution to the pleasurable servitude. As Solove notes in *Privacy Self-Management and the Consent Dilemma*, "privacy self-management is certainly a laudable and necessary component of any regulatory regime."³⁴⁸ And while flawed, privacy self-management is a widely accepted

345. An opt-in regime would seem preferable to an opt-out regime in preventing the commoditizing of identity but is less likely from a political perspective. It is unlikely a significant number of social media users would opt-in to such a regime to allow this form of identity-based advertising to remain profitable for advertisers and the social media platform. On the other hand, a significant percentage of social media users would likely not bother to opt-out.

346. Solove, *Consent Dilemma*, *supra* note 23, at 1883.

347. Hartzog, *supra* note 39, at 21.

348. Solove, *Consent Dilemma*, *supra* note 23, at 1880; *see also* Tuukka Lehtiniemi and Yki Korttesniemi, *Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary*

aspect of privacy regulation.³⁴⁹ Through privacy self-management regimes, the law seeks to give people control over their data by focusing on acquiring their consent.³⁵⁰ Indeed, privacy policies have certain advantages over more “paternalistic regulation.”³⁵¹

Nonetheless, privacy self-management is a flawed and incomplete solution as it is tasked with “doing work beyond its capabilities” and “does not provide people with meaningful control over their data.”³⁵² Solove highlights a few reasons why. First, humans have cognitive limitations which impair their ability to “make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data.”³⁵³ Second, privacy self-management does not scale well—“[t]here are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity.”³⁵⁴ And third, privacy self-management “addresses privacy in a series of isolated transactions guided by particular individuals. Privacy costs and benefits, however, are more appropriately assessed cumulatively and holistically—not merely at the individual level.”³⁵⁵

Are these shortcomings applicable to publicity self-management via publicity policies? Yes and no. The first point, regarding cognitive limitations, certainly is applicable. The second and third points, however, are perhaps less of an issue as to publicity. Consider that there are far fewer entities (i.e., primarily social media platforms) who seek publicity licenses or waivers than collect other aspects of personal data. Thus, although with respect to privacy, “[i]t is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses,”³⁵⁶ publicity licenses are less ubiquitous on the internet, and uses of user publicity are more narrowly

approach, *Big Data & Society*, July–December 2017 at 10 (concluding “that it is indeed possible to make privacy self-management work better, and some of its obstacles seem to be even solvable with new tools”); Mario Pascalev, *Privacy exchanges: restoring consent in privacy self-management*, 19 *Ethics and Information Technology* 39, 39 (2017) (arguing that a streamlined, automated, and standardized form of privacy self-management could be workable).

349. Solove, *Consent Dilemma*, *supra* note 23, at 1883.

350. Solove, *Consent Dilemma*, *supra* note 23, at 1880 (explaining that under a privacy self-management regime, “[c]onsent legitimatizes nearly any form of collection, use, or disclosure of personal data”).

351. Solove, *Consent Dilemma*, *supra* note 23, at 1903 (“Privacy self-management cannot achieve the goals demanded of it, and it has been pushed beyond its limits. But privacy self-management should not be abandoned, and alternatives risk becoming too paternalistic.”).

352. Solove, *Consent Dilemma*, *supra* note 23, at 1880-81.

353. Solove, *Consent Dilemma*, *supra* note 23, at 1880-81.

354. Solove, *Consent Dilemma*, *supra* note 23, at 1881.

355. Solove, *Consent Dilemma*, *supra* note 23, at 1881.

356. Solove, *Consent Dilemma*, *supra* note 23, at 1881.

tailored to advertising, marketing, and endorsements. Because publicity licenses are less common and thus publicity management less of a complexity for users, publicity policies coupled with an opt-out regime may be more effective than privacy self-management has been.

Like with privacy, though, the law may ultimately need to venture into substantive publicity rules beyond self-management to combat the pleasurable servitude. Such laws could consist of “hard boundaries,” affirmatively restricting publicity rights transfer (at least absent a heightened form of consent), in addition to “softer default rules” that could be bargained around, such as an opt-in (rather than opt-out) regime where users would need to toggle the default settings to allow for publicity licensure.³⁵⁷ Notably, prohibiting outright the transfer of publicity rights—in effect holding the right of publicity to be inalienable—risks stifling internet entrepreneurs (i.e., influencers) who seek to profit financially in part through publicity rights licensure.³⁵⁸ Ironically, hindering such entrepreneurial efforts may negatively impact autonomy while attempting to protect it.³⁵⁹ Regardless of how this balance is grappled with down the line, however, publicity policies, in drawing attention and education to the pleasurable servitude, provide a sound introductory step to a publicity regulatory regime.

C. FIRST AMENDMENT BALANCE

Laws regulating the pleasurable servitude should not necessarily implicate the First Amendment because identity-based sponsorship and endorsements are purely commercial activity. As discussed earlier in Section III.C, the right of publicity can clearly encroach on the First Amendment rights of creators. Thus, the First Amendment can, at least in cases of noncommercial speech, serve as a complete defense to publicity infringement.³⁶⁰ In the celebrity context, the First Amendment is often considered a public interest-oriented limit on an ever-expanding right of publicity.³⁶¹ As Post and Rothman put it, “[t]hose who wish to create expressive works that incorporate the identities of actual people, or who wish to post images and comments about actual people

357. Solove, *Consent Dilemma*, *supra* note 23, at 1903 (“[S]ubstantive rules about data collection, use, and disclosure could consist of hard boundaries that block particularly troublesome practices as well as softer default rules that can be bargained around.”).

358. Solove, *Consent Dilemma*, *supra* note 23, at 1881 (remarking that “although extensive self-exposure can have disastrous consequences, many people use social media successfully and productively.”); <https://www.traverselegal.com/blog/influencer-brand-and-agency/> (explaining that “[l]icensing of copyrights and publicity rights are the foundation of [the influencer] business”).

359. Solove, *Consent Dilemma*, *supra* note 23, at 1894.

360. *See, e.g.*, Tune & Levine, *supra* note 25, at 17-18.

361. *See supra* note 165 and accompanying discussion.

online, are bereft of reliable and foreseeable protection for the exercise of essential First Amendment rights.”³⁶²

Thus, where the appropriation of an individual’s identity relates to expressive works or has a social purpose other than purely commercial benefit (i.e., newsworthiness, parody, etc.), the First Amendment should serve as a complete defense to a right of publicity challenge.³⁶³ Yet, to the extent that a right of publicity challenge amounts to no more than the appropriation of one’s economic value, such purely commercial speech need not be protected expression under the First Amendment.³⁶⁴ Courts never (or almost never) conduct a four-part *Central Hudson* commercial speech inquiry where the right of publicity is at issue, instead preferencing the right of publicity over commercial speech as essentially a per se rule.³⁶⁵

In considering these guidelines, unlike with expressive works in the celebrity publicity context where it is strong, the First Amendment should serve as a weak defense in the pleasurable servitude cases. Because the use of identities for advertising and endorsement purposes in the social media marketing cases fits quite easily in the category of commercial speech, such use is thus outside the realm of historic core First Amendment protection, particularly as applied to the right of publicity.³⁶⁶ However, that is not a given considering the trend toward First Amendment expansionism in the last half century.³⁶⁷ As Tim Wu puts it, “[o]nce the patron saint of protesters and the disenfranchised, the First Amendment has become the darling” of economic

362. Post & Rothman, *supra* note 14, at 90-91.

363. Tune & Levine, *supra* note 25, at 17-18.

364. Tune & Levine, *supra* note 25, at 17-18; cf. Jennifer E. Rothman, *Commercial Speech, Commercial Use, and the Intellectual Property Quagmire*, 101 VIRGINIA L. REV. 1929, 2008 (2015) (arguing that the commercial versus non-commercial distinction is an insufficient binary from which to decide the availability of a First Amendment defense in intellectual property matters).

365. *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. 557, 566 (1980) (describing a four-part analysis for evaluating restrictions on commercial speech); Martin H. Redish & Kelsey B. Shust, *The Right of Publicity and the First Amendment in the Modern Age of Commercial Speech*, 56 WM. & MARY L. REV. 1443, 1478-79 (2015) (“[T]he paucity of judicial decisions applying the Supreme Court’s famed four-part *Central Hudson* test to determine the appropriate protection for speech relative to publicity rights claims is astounding.”).

366. *But see Sorrell v. IMS Health Inc.*, 546 U.S. 552 (2011) (striking down on First Amendment grounds a commercial speech regulation involving a Vermont law that prevented pharmacies from selling data that would show the prescription patterns of doctors).

367. Redish & Shust, *supra* note 365, at 1450 (arguing that “commercially motivated expression is appropriately extended the same level of First Amendment protection against right of publicity claims as traditionally protected expression receives.”).

libertarians and corporate lawyers who have recognized its power to immunize private enterprise from legal restraint.”³⁶⁸

As an example, consider Facebook’s specious argument in *Fralely* that “[b]ecause the expressive modes of sharing that can lead to a Sponsored Story are ‘inextricably intertwined’ with the ‘commercial aspects’ of a Sponsored Story, any constraint on Facebook’s rebroadcast of these stories would likely run afoul of the First Amendment.”³⁶⁹ Under Facebook’s argument, Sponsored Stories are newsworthy matters of public interest because they are “expressions of commercial opinion.”³⁷⁰ Facebook’s rhetoric is a stretch, though, because the social network’s real motivation is strictly commercial gain.³⁷¹ That is, Facebook’s speech is “related solely to the economic interests of the speaker and its audience”³⁷² and “does no more than propose a commercial transaction.”³⁷³

In fact, First Amendment protections, particularly in the realm of commercial speech, are a relatively recent advent. For much of American history, the First Amendment “sat dormant.”³⁷⁴ In the 1920s, it began protecting “political speech” in earnest due to the federal government’s speech control programs and extensive propaganda during the First World War.³⁷⁵ Beginning in the 1950s, the First Amendment began to be used to protect speech that is less overtly political, such as indecency and cultural expression.³⁷⁶ In 1976, with *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*,³⁷⁷ it was extended to cover commercial advertising, far beyond “the kind

368. Tim Wu, *The Right to Evade Regulation*, NEW REPUBLIC (June 3, 2013) (discussing the phenomenon of “[h]ow corporations hijacked the First Amendment”), <https://newrepublic.com/article/113294/how-corporations-hijacked-first-amendment-evade-regulation>.

369. Def. Facebook, Inc.’s Brief in Supp. Of Pls.’ Mot. For Prelim. Approval of Settlement, Case No. 11-CV-01726 LHK (PSG), <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1131&context=historical> (citing *Riley v. Nat’l Fed’n of the Blind*, 487 U.S. 781, 796 (1988); *Hoffman v. Capital Cities/ABC, Inc.*, 255 F.3d 1180, 1185 (9th Cir. 2001)).

370. *Id.*

371. *See* *Downing v. Abercrombie & Fitch*, 265 F.3d 994, 1002 (9th Cir. 2001) (holding that noncelebrity plaintiff’s surfing photo being used in a clothing catalog was not a matter of public interest given the strictly commercial interests at stake).

372. *See* *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. 557, 561 (1980).

373. *Bolger v. Youngs Drug. Prods. Corp.*, 463 U.S. 60, 66 (1983).

374. Tim Wu, *Is the First Amendment Obsolete?*, 117 MICH. L. REV. 547, 551 (2018) (noting that the First Amendment “is an American tradition in the sense that the Super Bowl is an American tradition—one that is relatively new, even if it has come to be defining.”).

375. *Id.*

376. *See* *Roth v. United States*, 354 U.S. 476 (1957).

377. *Va. State Bd. Of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748, 772-73 (1976).

of political and press activity that was the original concern of those who brought the First Amendment to life.”³⁷⁸ And in 2011, in *Sorrell v. IMS Health, Inc.*, commercial speech protection under the First Amendment was further extended to the creation and dissemination of data.³⁷⁹

To the extent internet platforms use the First Amendment as a defense in right of publicity cases like *Fraleigh*, *Perkins*, and *Dancel*, or to challenge prospective endorsement-based regulations on the pleasurable servitude, such tactics are instances of what Charlotte Garden calls the “deregulatory First Amendment.”³⁸⁰ This refers to the Supreme Court’s now decades-long expansion of First Amendment protection of commercial speech and of limiting economic regulations.³⁸¹ Jurists and scholars have compared this deregulatory agenda—the “hijacking” of the First Amendment by corporations—to the judicial excesses of the *Lochner* era.³⁸² In this sense, some have challenged the claim that data privacy laws and other regulations on information are necessarily speech that restrict the dissemination of truthful information and thus violative of the First Amendment.³⁸³ As applied to the online publicity licensing phenomenon, the First Amendment defense becomes a tool for internet platforms to evade liability rather than a serious

378. Wu, *supra* note 374, at 553.

379. *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 580 (2011)

380. See generally Charlotte Garden, *The Deregulatory First Amendment at Work*, 51 HARV. C.R.-C.L. L. REV. 323 (2016) (coining the term “deregulatory First Amendment” to describe the phenomenon of its expansionism into protecting commercial speech” and applying it in the context of labor and employment law, hence the article title’s double entendre).

381. *Sorrell*, 546 U.S. at 587 (Breyer, J., dissenting) (noting that regulatory actions of the kind present here [concerning information disclosures] have not previously been thought to raise serious additional constitutional concerns under the First Amendment.”); Shaun Spencer, *Two First Amendment Futures: Consumer Privacy Law and the Deregulatory First Amendment*, 2020 MICH. ST. L. REV. 897, 900 (2021) (explaining that in the consumer privacy context, there is greater deregulatory potential because data flows “bear[] a superficial resemblance to speech”).

382. *Sorrell*, 564 U.S. at 591 (arguing that expansive free speech jurisprudence “return[s] constitutional law] to the bygone [Lochner] era”) (Breyer, J., dissenting); Wu, *supra* note 368; cf. Genevieve Lakier, *The First Amendment’s Real Lochner Problem*, 87 U. CHI. L. REV. 1241, 1342 (2020) (“There are significant and important similarities between Lochner-era due process jurisprudence and contemporary free speech law—albeit, not the similarities that most contemporary critics point to.”). *Lochner* is in reference to the infamous *Lochner v. New York*, 198 U.S. 405 (1905), which enforced an unconscionable freedom to contract despite situations of vastly unequal bargaining power, and heralded what many consider to be the dystopian “Lochner era” of the U.S. Supreme Court.

383. See, e.g., Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1151 (2005) (challenging “the conventional wisdom that regulating databases regulates speech, that the First Amendment is thus in conflict with the right of data privacy, and that the Constitution thereby imposes an insuperable barrier to basic efforts to tackle the database problem.”).

defender of free speech. Courts are not forced through binding precedent to give credence to such a corrupting deregulatory First Amendment agenda and should not do so.

Scholars often believe that curbing the excesses of the “extravagant,”³⁸⁴ “bloated monster”³⁸⁵ that is the right of publicity in exchange for free speech is an obvious choice. And perhaps it is in the celebrity publicity context. But in drawing attention to the pleasurable servitude, which affects mostly everyday citizens, jurists and commentators should think twice about trading citizens’ identity-based protections in exchange for a romanticized notion of the First Amendment.³⁸⁶ In the context of the pleasurable servitude, the First Amendment defense is the constitutional extravagance, rather than the ordinary citizen’s right of publicity.³⁸⁷ This weakened First Amendment defense, though, makes the consent defense even more important for internet platforms, hence their compulsory licensing of users’ publicity rights via the pleasurable servitude.

V. CONCLUSION

*After all, every one belongs to every one else.*³⁸⁸

The concept of “identity” is a largely metaphysical subject. But for purposes of the right of publicity—“the right of every human being to control the commercial use of his or her identity”³⁸⁹—the law must grapple with the question of what constitutes identity and the harms flowing from its transfer. Literary metaphors help conceptualize ethereal subject matter such as the

384. Stacey Dogan, *Stirring the Pot: A Response to Rothman’s Right of Publicity*, 42 Colum. J.L. & Arts 321, 329 (2019).

385. ROTHMAN, RIGHT OF PUBLICITY, *supra* note 15 at 7 (2018).

386. See *Janus v. Am. Fed’n of State, Cty., & Mun. Emps., Council 31*, 138 S. Ct. 2448, 2501 (2018) (Kagan, J., dissenting) (accusing majority of “weaponizing the First Amendment” in overturning long-standing precedent requiring public-sector employees to pay union fees).

387. Marlan, *supra* note 15, at 463–68. Here, invocation of the First Amendment appears to be standing in for a broader public domain claim for the free use of human identity—name, image, and likeness. But the romance of the public domain “obscures the distributional consequences of [that commons].” See Anupam Chander & Madhavi Sunder, *The Romance of the Public Domain*, 92 CAL. L. REV. 1331, 1334 (2004). In a similar vein as other intellectual property rights, this romance of the First Amendment obscures the distributional inequities inherent in the right of publicity context too. See Jamar & Mtima, *supra* note 168, at 13 ([b]ecause of institutionalized barriers to information, financial capital, and legal support, many members of marginalized communities have been unable to commercially develop and exploit their publicity rights, while majority enterprises have proven quite adept at exploiting these properties.”).

388. HUXLEY, *supra* note 8, at 50.

389. MCCARTHY & SCHECHTER, *supra* note 7.

subjective harms inflicted by a lack of privacy in our surveillance age. To this end, dystopian metaphors like Orwell's Big Brother, in focusing on power and control, and other surveillance metaphors, like Kafka's *The Trial*, in focusing on a shadowy bureaucracy, are useful where a literal analysis falls short.³⁹⁰ Finding appropriate metaphors is thus essential to framing *privacy* problems and for the development of sound legislation.³⁹¹

The right of *publicity*, though, has no such prevailing conceptual metaphor (aside from the term "publicity" itself, which connotes fame and celebrity). Therefore, many remain in the dark about this personality right and the extent of the harms flowing from its manipulation. Yet the right of publicity has the potential both to be exploited, as well as to act as a safeguard in our data-driven age. The *Brave New World* metaphor—in depicting a society built around both (1) entertainment as a form of control and (2) socially conditioned technological manipulation—gets at the fact that the right of publicity is a two-tiered right.

On one hand, the right of publicity is an extravagant right focused on protecting celebrities—the rich and famous "stars" of our society. This conventional notion of the right of publicity, was formulated at a time (the 1950s) when there existed a strict bifurcation between famous people and non-famous people. This celebrity-focused right has the potential to chill the First Amendment rights of creators who portray real famous people, including for purposes of public discourse. On the other hand, the right of publicity is a *right to identity* that many regular citizens have stripped away by agreeing to technology corporations' draconian terms of service required to use social media and other online services. In the pleasurable servitude context, the First Amendment presents less of a conflict, because social networks use of identities is for advertising, sponsorships, and endorsements—what should be a clear-cut form of commercial speech, the likes of which are routinely trumped by the right of publicity.

The need to curtail the celebrity-focused right to ensure First Amendment protections is a well-documented publicity problem. But the pleasurable servitude—the voluntary licensing of social media users' rights of publicity as a prerequisite for use of the platforms—should drive regulation in this area

390. See Solove, *Privacy and Power*, *supra* note 3, at 1398 (arguing that problems with mass data collection are best captured by "Franz Kafka's depiction of bureaucracy in *The Trial*—a more thoughtless [than Big Brother] process of bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable...").

391. Kaplan, *supra* note 2 ("The battle of the metaphors is much more than a literary parlor game The way a problem is framed determines its solution The right metaphor is a necessary ingredient to good legislation.").

given the overwhelming frequency with which it occurs on the internet and social media. The right of publicity's transferability is a problem in this regard, as is the questionable level of consent needed for its alienation from identity holders. Hence this Article's proposal of publicity policies analogous to privacy policies.

The conceptualization of online publicity licenses as a "pleasurable servitude" underscores the perniciousness of such agreements on an individual's right to publicity. Seen through the lens of *Brave New World*, the right of publicity is not only a First Amendment problem as in the case of celebrity publicity but also a consent dilemma for ordinary citizens in the social media context. The pleasurable servitude involves technological manipulation, social conditioning, human commodification, and ultimately the loss of identity rights at the hands of online social media platforms, who operate as powerful quasi-governments. Increasingly, though, we find such servitude delightful, which is just the sort of dystopian nightmare Huxley warned against in *Brave New World*.

TRADEMARK CONFUSION SIMPLIFIED: A NEW FRAMEWORK FOR MULTIFACTOR TESTS

Daryl Lim[†]

ABSTRACT

Multifactor tests are challenging for judges to apply consistently and accurately. Poorly done, they could result in law without order. How courts determine trademark infringement provides a case study for what experimental psychology and artificial intelligence can offer to reduce bias and variability in multifactor tests. In trademark law, judges must determine the likelihood of consumer confusion to decide whether a mark infringes upon a trademark holder’s rights. Plenty of commentaries have criticized the likelihood of confusion tests, but none offer a comprehensive analysis linking the impact of the legal standard’s disorder with the root causes of that disfunction. Likewise, none demonstrate how doctrine and technology can work hand in glove to simplify this puzzling standard.

This Article draws on empirical studies, case law, and the latest experimental psychology and artificial intelligence literature to shift the debate from critiquing to simplifying the likelihood of confusion standard. It explains how three core factors, combined with two safe harbors and today’s deep learning algorithms enable courts to reach consistent and accurate results. The simplified framework will promote fair play, safeguard expressive uses, and enhance access to justice. These takeaways apply more broadly and address defects common to multifactor tests.

TABLE OF CONTENTS

I. INTRODUCTION	868
II. VARIABILITY AND BIAS OFTEN UNDERLY MULTIFACTOR TESTS.....	872

DOI: <https://doi.org/10.15779/Z38G737509>.

© 2022 Daryl Lim.

[†] This manuscript benefited from the author’s participation in the twenty-eighth Fordham IP Conference, Giles S. Rich Inn IP American Inn of Court and Pauline Newman IP American Inn of Court Seminar, and World IP Forum. Invited presentations for takeaways featured in this Article include the Indiana University (Bloomington) IP Colloquium, the George Mason University Antonin Scalia Law School C-IP2 Ninth Annual Fall Conference, and the American IP Law Association Emerging Technology Committee and Electronic and Computer Law Committee Roadshow. Professors Jon Lee, Joshua Sarnoff, and Peter Yu provided valuable comments and suggestions. My sincere thanks to Sarah Davidson, Justine McCarthy Potter, Breanna Qin, and Sophia Wallach at the Berkeley Technology Law Journal for their meticulous and helpful editorial assistance.

III. INSIDE TRADEMARK'S BLACK BOX: THE LIKELIHOOD OF CONFUSION.....	878
A. FROM BRAND EQUITY TO BABEL	879
B. THE LANHAM ACT AND THE LIKELIHOOD OF CONFUSION.....	881
C. THE CASE FOR CLARITY	886
IV. ROOTS OF CONFUSION	892
A. EXPANSION INTO CONFUSION.....	892
1. <i>Blending the Law on Trade Names and Trademarks</i>	892
2. <i>Yet More Triggers for Confusion</i>	896
B. AN INTENT TO CONFUSE	897
C. TRADEMARK'S AUDIENCE.....	901
1. <i>Surveys are Expensive and Misleading</i>	902
2. <i>Trademark Strength is Not the Answer</i>	905
3. <i>Consumer Sophistication is not the Answer</i>	907
D. ADDRESSING COHERENCE-BASED REASONING	908
V. RULES OF THUMB.....	913
A. TRADEMARK'S TROIKA	913
B. SAFE HARBORS.....	916
C. POWERED BY ARTIFICIAL INTELLIGENCE: HOW TO CATALYZE TRADEMARK REFORM PROPERLY	920
1. <i>Predictive Analytics</i>	923
2. <i>The Robot Judge</i>	927
3. <i>Weighing the Troika Factors</i>	929
D. COURTS, NOT CONGRESS.....	931
VI. RULES, STANDARDS, AND SAFE HARBORS.....	932
VII. CONCLUSION.....	937

I. INTRODUCTION

Deploying multifactor tests accurately and consistently is a challenging business. Courts produce judgments, not computations, and legal doctrine leaves room for varying interpretations and dissents.¹ Even judges who agree on doctrine may differ on how they apply it.² The two reasons for these

1. See generally Daryl Lim, *I Dissent: The Federal Circuit's "Great Dissenter," Her Influence on the Patent Dialogue, and Why It Matters*, 19 VAND. J. ENT. & TECH. L. 873, 883–90 (2020) (explaining why judges dissent).

2. *Id.*

differences are bias, which consistently leads to the wrong outcome, and noise which leads to inconsistent outcomes.³ Both harm the legal system's credibility.⁴

Neither noise nor bias may be obvious to the casual observer. Judges are recognized experts in the law and dazzle us with their opinions.⁵ Moreover, much of the variability in their judgments is intentional. Judges use majorities and dissents as a means to endorse the judgments most worthy of support.⁶ Judgments would also be of little value if they were all identical regardless of the facts. However with variability comes the risk of noise and bias.

The literature is replete with the dangers of bias in the law.⁷ Even those who believe in the value of individualized judgments will agree: variability that turns judgment into a lottery becomes unjust. Something must have gone badly wrong if one defendant for the same offense gets jail time and another gets a mere warning. These errors do not cancel out, and justice has not, on average, been served. Instead, they add up.

The tensions caused by variability and bias exist whenever the law must choose between standards and rules.⁸ Rules provide certainty but come at the expense of rigidity and over- or underinclusiveness.⁹ Conversely, standards can be more flexible but are less predictable.¹⁰ Trademark infringement provides a useful case study to examine how this happens and, more importantly, how society can fix it. As the fulcrum of trademark law, the entire infringement inquiry rests on courts determining the nature and scope of likelihood of confusion (“LOC”) appropriate for each new set of facts. Conversely,

3. *See generally* DANIEL KAHNEMAN, CASS SUNSTEIN & OLIVIER SIBONY, NOISE: A FLAW IN HUMAN JUDGEMENT 259 (2021) (discussing bias and noise).

4. *See infra* Part II.

5. *See* KAHNEMAN ET AL., *supra* note 3, at 228 (“The confidence heuristic points to the fact that in a group, confident people have more weight than others, even if they have no reason to be confident.”).

6. *See* Lim, *supra* note 1, at 875.

7. *See, e.g.*, Daryl Lim, *Retooling the Patent-Antitrust Intersection: Insights from Behavioral Economics*, 69 BAYLOR L. REV. 124, 155–75 (2017) (collecting sources in the context of patent and antitrust law).

8. *See, e.g.*, Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685, 1687–1713 (1976); Carol M. Rose, *Crystals and Mud in Property Law*, 40 STAN. L. REV. 577, 592–93 (1988).

9. *See infra* Parts II and VI.

10. *See infra* Parts II and VI.

addressing the tension in trademark's LOC standard has spillover benefits for other areas of the law as well.¹¹

Trademarks envelop our senses both online and in the real world, blending a bouquet of information for our senses.¹² Businesses imbue words, symbols, scents, and sounds with information about their goods and services.¹³ Consumers lean on these imbued signs, routinely making snap judgments about the price and quality of products or services without detailed inquiry.¹⁴ Coffee aficionados seek out Starbucks' famous green mermaid, and viewers of dance, lip-sync, or comedy videos find TikTok's stylized treble clef. Businesses who attain cult statuses like Apple or Tesla imbue even untested product lines with a halo of desirability.¹⁵ This desirability may enable them to expand rapidly into adjacent markets.

When trademark owners, seeking to protect their trademarks, enforce their rights, courts apply the LOC standard to determine whether consumers would likely be confused by the defendants' use of their mark. The standard, which involves a multifactor test, lies at the heart of trademark law.¹⁶ Judges first identify and discuss evidence relevant to each factor before concluding if that factor weighs in favor of a likelihood of confusion between the two marks.¹⁷ They then make a holistic assessment from the perspective of the ordinary consumer in the marketplace.¹⁸ In practice this assessment manifests itself as a weighing of the factors the court earlier identified as being relevant in the LOC analysis.¹⁹

The LOC standard is a jurisprudential black hole.²⁰ It remains poorly theorized, and opinions on the standard usually fail to explain their decisions

11. See *infra* Part VI. Likelihood of confusion examines whether there is a substantial risk consumers will be confused as to the source, identity, sponsorship, or origin of the defendants' goods.

12. 15 U.S.C. § 1127 (“The term ‘trademark’ includes any word, name, symbol, or device, or any combination thereof . . . [used] to identify and distinguish . . . goods.”).

13. See 4 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 3, at 1 (4th ed. 1994).

14. *Qualitex Co. v. Jacobson Prods. Co.*, 514 U.S. 159, 163–64 (1995) (“[T]rademark law . . . reduces the customer’s costs of shopping and making purchasing decisions, . . . for it quickly and easily assures a potential customer that this item—the item with this mark—is made by the same producer as other similarly marked items that he or she liked (or disliked) in the past.”).

15. See Jennifer L. Aaker, *Dimensions of Brand Personality*, 34 J. MKTG. RES. 347, 348 (1997).

16. See *infra* Part III.

17. See, e.g., *In re E. I. Du Pont de Nemours & Co.*, 476 F.2d 1357, 1361 (C.C.P.A. 1973).

18. See generally MCCARTHY, *supra* note 13, § 23:1.

19. See e.g., *Disney Enters., Inc. v. Sarelli*, 322 F.Supp.3d 413, 438–39 (2018).

20. See *infra* Part III.

in a way courts can easily apply.²¹ Moreover, each outcome is fact-specific, limiting transferrable principles from circuit to circuit and from one part of trademark law to another.²²

Plenty of commentaries have criticized the LOC standard.²³ Yet none offer a comprehensive analysis connecting the impact of confusion on stakeholders, the root causes of that confusion, or solutions based on foundational trademark doctrine and forward-looking technology. This Article fills a gap in the literature as scholars fail to devise laws integrating the advantages of rules and standards while minimizing their shortcomings. Rather than displacing the LOC standard, this Article explains how a simplified, artificial intelligence (AI)-enabled standard provides a superior threshold for infringement. In doing so, this general purpose approach provides a roadmap for refining other multifactor tests, helping them produce more reliable and precise judgments.

Specifically, this Article draws on empirical studies, case law, experimental psychology, and AI literature to shift the debate from critiquing to simplifying the LOC standard. It unearths the roots of confusion²⁴ and explains how (1) three overlooked factors, combined with (2) two safe harbors and (3) AI techniques available today, can work together to help courts and parties cut through bias and noise to reach consistent and accurate results.²⁵ The “Troika” factors and the safe harbors create “rules of thumb,” which, when AI enables them, go far beyond trademark law to promote commercial fair play, safeguard expressive uses, and enhance access to justice in other multifactor tests, including those used in civil procedure, consumer information law, conflict of laws, copyright, criminal, and constitutional law.²⁶

Despite the urging of appeals courts, lower court judges do not approach multifactor tests robotically or discretely. Instead of using interrelated analysis, they sum up a few factors on a mental ledger as a strategy for navigating complexity. In effect, these tests become mere smokescreens for judges to create the appearance of coherence by resting on a small number of probative factors. Thus, the key to simplifying confusion in the case law, and thereby facilitating the creation of more consistent and accurate results, is to

21. See *infra* Part IV; see also Barton Beebe, *An Empirical Study of the Multifactor Tests for Trademark Infringement*, 94 CALIF. L. REV. 1581, 1582 (2006) (“Its current condition is Babelian.”).

22. See *infra* Section IV.B (“Trademark litigation is inherently impressionistic, particularly when actual confusion is rare.”).

23. See, e.g., *infra* Section IV.B (in the context of the intent factor).

24. See *infra* Section IV.A–B.

25. See *infra* Section IV.C.

26. See *infra* Part V.

concentrate the standard on a few factors and help judges use those factors well.

II. VARIABILITY AND BIAS OFTEN UNDERLY MULTIFACTOR TESTS

The adage that “beauty is in the eye of the beholder” suggests that people will naturally differ if there is more than one perspective. A cloud of possibilities exists wherever there is judgment, even in a seemingly unique situation, driven by biases and inconsistency.²⁷ As people pick different pieces of evidence to form the core of their narrative, they reach different conclusions.

Sometimes these choices lead to unfair decisions. For example, two judges who reviewed similar refugee asylum cases in the same Miami courthouse granted asylum at dramatically different rates. One judge granted refugees asylum in eighty-eight percent of cases, while the other did so only five percent of the time.²⁸ And in a large-scale study, fifty judges from various districts across the country were given identical presentence reports based on hypothetical cases and were asked to set sentences for the hypothetical defendants.²⁹ The study found that the “absence of consensus was the norm.”³⁰

An absence of consensus exacerbates vagueness in the law when Congress delegates wide discretionary powers to the courts. For instance, antitrust standards suffer from a similar openendedness problem as outcomes are driven less by doctrine and more by ideology.³¹ The same is true for constitutional law.³² The danger is that through the lens of the rule of law, indeterminable laws expand the government’s opportunities for corruption and tyranny and may overempower the government or those leveraging on

27. See KAHNEMAN ET AL., *supra* note 3, at 39-43.

28. Jaya Ramji-Nogales, Andrew I. Schoenholtz & Philip G. Schrag, *Refugee Roulette: Disparities in Asylum Adjudication*, 60 STAN. L. REV. 295, 296 (2007).

29. ANTHONY PARTRIDGE & WILLIAM B. ELDRIDGE, THE SECOND CIRCUIT SENTENCE STUDY: A REPORT TO THE JUDGES OF THE SECOND CIRCUIT (Federal Judicial Center, Aug. 1974).

30. *Id.* at 9. A heroin dealer could be jailed for one to ten years. A bank robber could be jailed five to eighteen years. *Id.* at 6.

31. See generally, Marina Lao, *Ideology Matters in the Antitrust Debate*, 79 ANTITRUST L.J. 649, 651-52 (2014) (“Arguments in contemporary antitrust are not merely technical but stem from ideological differences between antitrust conservatives and antitrust liberals concerning the economy and markets and the appropriate role of government within them, the virtues of dominant firms, the value of competition, and related social and political issues.”).

32. See Kermit Roosevelt III, *Constitutional Calcification: How the Law Becomes What the Court Does*, 91 VA. L. REV. 1649, 1665 (2005) (“a court may substitute a decision rule that turns on objective and easily ascertainable factors.”).

vague rules to extract concessions during settlements.³³ To prevent legislatures from outlawing behaviors in broad terms that fails to provide fair notice, constitutional law voids such laws for vagueness.³⁴

On the other hand, having too many rules interwoven into the law also create its own set of problems. Consider how courts must routinely apply numerous factors, each potentially carrying different weights for different judges. For example, damages and lost profits in patent law require judges to balance fifteen *Georgia-Pacific* factors and four *Panduit* factors, respectively.³⁵

33. See Cass R. Sunstein, *Problems with Rules*, 83 CALIF. L. REV. 953, 968–69 (1995) (arguing rules are necessary to prevent arbitrary enforcement). See also *infra* Part II.

34. John F. Decker, *Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws*, 80 DENV. U. L. REV. 241, 248 (2002) (“A statute is void for vagueness if it fails to draw reasonably clear lines between lawful and unlawful conduct such that the defendant has no way to find out whether his conduct is controlled by the statute. Vague statutes are constitutionally unacceptable because they fail to provide citizens with fair notice or warning of statutory prohibitions so that they may act in a lawful manner.”).

35. See *Georgia-Pacific Corp. v. U. S. Plywood Corp.*, 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970)

- (“1. The royalties received by the patentee for the licensing of the patent in suit, proving or tending to prove an established royalty.”)
2. The rates paid by the licensee for the use of other patents comparable to the patent in suit.
3. The nature and scope of the license, as exclusive or non-exclusive; or as restricted or non-restricted in terms of territory or with respect to whom the manufactured product may be sold.
4. The licensor's established policy and marketing program to maintain his patent monopoly by not licensing others to use the invention or by granting licenses under special conditions designed to preserve that monopoly.
5. The commercial relationship between the licensor and licensee, such as, whether they are competitors in the same territory in the same line of business; or whether they are inventor and promoter.
6. The effect of selling the patented specialty in promoting sales of other products of the licensee; that existing value of the invention to the licensor as a generator of sales of his non-patented items; and the extent of such derivative or convoyed sales.
7. The duration of the patent and the term of the license.
8. The established profitability of the product made under the patent; its commercial success; and its current popularity.
9. The utility and advantages of the patent property over the old modes or devices, if any, that had been used for working out similar results.
10. The nature of the patented invention; the character of the commercial embodiment of it as owned and produced by the licensor; and the benefits to those who have used the invention.

Determining copyright ownership in work-for-hire cases requires owners to canvass eleven factors.³⁶ Similar issues permeate consumer information law,³⁷ First Amendment law,³⁸ and the proportionality of punishment under the Eighth Amendment.³⁹

-
11. The extent to which the infringer has made use of the invention; and any evidence probative of the value of that use.
 12. The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the invention or analogous inventions.
 13. The portion of the realizable profit that should be credited to the invention as distinguished from non-patented elements, the manufacturing process, business risks, or significant features or improvements added by the infringer.
 14. The opinion testimony of qualified experts.
 15. The amount that a licensor (such as the patentee) and a licensee (such as the infringer) would have agreed upon (at the time the infringement began) if both had been reasonably and voluntarily trying to reach an agreement; that is, the amount which a prudent licensee—who desired, as a business proposition, to obtain a license to manufacture and sell a particular article embodying the patented invention—would have been willing to pay as a royalty and yet be able to make a reasonable profit and which amount would have been acceptable by a prudent patentee who was willing to grant a license.”); *Panduit Corp. v. Stahl Bros. Fibre Works, Inc.*, 575 F.2d 1152, 1164 (6th Cir. 1978) (identifying (1) demand for the patented product, (2) absence of acceptable non-infringing alternatives, (3) manufacturing and marketing capability to exploit the demand, and (4) the amount of profit the plaintiff would have made).

36. *Cnty. Creative Non-Violence v. Reid*, 490 U.S. 730, 751–52 (1989) (“Among the other factors relevant to this inquiry are the skill required; the source of the instrumentalities and tools; the location of the work; the duration of the relationship between the parties; whether the hiring party has the right to assign additional projects to the hired party; the extent of the hired party’s discretion over when and how long to work; the method of payment; the hired party’s role in hiring and paying assistants; whether the work is part of the regular business of the hiring party; whether the hiring party is in business; the provision of employee benefits; and the tax treatment of the hired party.”).

37. See Michael Grynberg, *More Than IP: Trademark Among the Consumer Information Laws*, 55 WM. & MARY L. REV. 1429, 1473 (2014) (“Key words like ‘likelihood,’ ‘confusion,’ and ‘approval’ are undefined, opening the door to judicial creativity and applications of the trademark cause of action to situations alien to its common law roots.”).

38. See Matthew D. Bunker, *Mired in Confusion: Nominative Fair Use in Trademark Law and Freedom of Expression*, 20 COMM. L. & POL’Y 191, 193–94 (2015) (“The multi-factor confusion approach embodied in *Sleekcraft* and similar tests creates many of the same problems generated by multi-factor tests in other areas of the law.”).

39. Dan Simon, *The Limited Diagnosticity of Criminal Trials*, 64 VAND. L. REV. 143, 177 (2011) (“These results are statistically better than flipping a coin, but barely so.”).

The key takeaway here is that less is more. Another psychology experiment showed that test subjects defaulted to a coin flip when they experienced factor overload.⁴⁰ Subjects had to apply either a nine-factor test, a zero-factor test, or a three-factor test to a set of facts.⁴¹ The control case was based on identical facts whose outcome was widely accepted as correct, providing a yardstick to evaluate whether the subjects' decisions were accurate.⁴² The study reported that the outcome under the nine-factors condition was similar to under the zero-factor condition. In contrast, subjects produced decisions closest to the widely accepted legal decision only under a three-factors condition.⁴³

Another problem in judicial decision-making is bias.⁴⁴ Bias is a problem that goes beyond the law. In one medical study assessing angiograms, physicians disagreed with their earlier judgments more than half the time.⁴⁵ Decision-makers may also substitute answering a difficult question by finding the answer to an easier one because of psychological biases.⁴⁶ For instance, replacing the question "Is there climate change?" with "Do I trust the people who say it is real?" introduces variability depending on the answerer's social circles, information sources, and political affiliation. These biases will lead to answers that fail to give the evidence their appropriate weights, resulting in judgment errors.⁴⁷

The good news is that biases and variability can be reduced by rethinking how we approach rules and standards. For instance, Congress enacted the Sentencing Reform Act of 1984 to issue mandatory guidelines and establish a restricted range for criminal sentences.⁴⁸ The new law was intended to reduce variability by reducing "the unfettered discretion the law confers on those judges and parole authorities responsible for imposing and implementing the sentences."⁴⁹

Previously, judges had to apply a standard that would otherwise differ on weights they assign to factors.⁵⁰ The 1984 Guidelines required judges to

40. *Id.*

41. *Id.*

42. *Id.*

43. Dan Simon, *A Third View of the Black Box: Cognitive Coherence in Legal Decision Making*, 71 U. CHI. L. REV. 511, 511 (2004) (finding that fewer conditions made the reason for the decision clearer and therefore it was easier for the subjects to determine the result).

44. *See* Lim, *supra* note 7.

45. Katherine M. Detre, Elizabeth Wright, Marvin Murphy & Timothy Takaro, *Observer Agreement in Evaluating Coronary Angiograms*, 52 CIRCULATION 979 (1975).

46. *See* KAHNEMAN ET AL., *supra* note 3, 164-67.

47. *See* KAHNEMAN ET AL., *supra* note 3, 164-67.

48. PUB. L. NO. 98-473, 98 STAT. 1987.

49. S. REP. NO. 225, 98th Cong., 2d Sess. 52, *as reprinted in* 1984 U.S.S.C.A.N. 3182, 3221.

50. *Id.*

consider two factors to establish sentences: the crime, and the number and severity of a defendant's previous convictions.⁵¹ Crimes are assigned one of forty-three "offense levels," depending on their seriousness, and judges have a narrow range of sentencing, with the top of the range authorized to exceed the bottom by the greater of six months or twenty-five percent.⁵² Judges could depart from the range by aggravating or mitigating circumstances, subject to appellate review.⁵³

When judges used the Guidelines, this made the sentence less dependent on the judge doing the sentencing.⁵⁴ The authors attributed the reduced variation to the Guidelines because guidelines break down vague standards into a few factors that are easier to understand. They arguably nudge judges to pay attention to variables that truly matter rather than biased or irrelevant factors. Ideally, as case law develops around the guidelines, courts will create a clear method for evaluating each factor, simplifying each factor-level judgment, and reducing its variability.

Refining how courts deploy rules and standards provides them and other legal stakeholders with a powerful benefit–predictability. A study on bail decisions used two inputs known to be highly predictive of a defendant's likelihood to jump bail: the defendant's age, as the elderly are lower flight risks, and the number of past court dates missed, as people who are flaky in appearing tend to recidivate.⁵⁵ The model translated these two inputs into several points, which data scientists used as a risk score.⁵⁶ This model outperformed virtually all human bail judges in predicting flight risk.⁵⁷ In all tasks, the model did as well as more complex regression models did but underperformed AI machine learning techniques.⁵⁸ When AI succeeds in this way, these models not only reduce bias and variability, but also allow courts to harness much more information. AI, then, provides the final piece of the new framework for multifactor tests.

51. *Id.*

52. *Id.*

53. U.S. SENT'G GUIDELINES MANUAL 7 (2018), www.ussc.gov/sites/default/files/pdf/guidelines-manual/2018/GLMFull.pdf.

54. James Anderson, Jeffrey Kling & Kate Stith, *Measuring Interjudge Sentencing Disparity: Before and After the Federal Sentencing Guidelines*, 42 J. LAW & ECON. 271, 303 (1999).

55. Jongbin Jung, Connor Concannon, Ravi Shroff, Sharad Goel & Daniel Goldstein, *Simple Rules to Guide Expert Classifications*, 183 J. ROYAL STAT. SOC'Y 771 (2020).

56. *Id.*

57. *Id.* When researchers applied the model to different context, they used up to five inputs (compared with the two used to predict flight risk) and weighted the different inputs by small whole numbers (between -3 and +3).

58. *Id.*

AI has revolutionized the legal practice in predicting doctrine,⁵⁹ with machine learning techniques enabling AI to forecast decisions of the US Supreme Court.⁶⁰ When there is a lot of data, machine learning algorithms may do better than humans, and better than simple rules.⁶¹ In this Article, I argue that AI works best in tandem with humans in deciphering trademark law's multifactor test for determining infringement, the LOC standard. AI-augmented decisionmaking can thus improve human judgment by using data science to identify how the facts map to each relevant factor, thereby reducing biases and variability in predictions and evaluations.⁶² As Daniel Kahneman, Cass Sunstein, and Olivier Sibony noted in their 2021 book *Noise*:

[A]lthough a predictive algorithm in an uncertain world is unlikely to be perfect, it can be far less imperfect than noisy and often-biased human judgment. This superiority holds in terms of both validity (good algorithms almost always predict better) and discrimination (good algorithms can be less biased than human judges).⁶³

Collectively, the foregoing offers a roadmap of the key points this Article will cover. First, legal standards force judges to do a lot of work to specify the meaning of open-ended terms, causing them to rely on irrelevant factors or get lost in multifactor tests. In addition to finding facts, courts must give content to relatively vague phrases like what is “reasonable,” “likely,” or amounts to “confusion.”⁶⁴ Too many rules also create confusion and unjustified variability. When judges themselves become confused, they introduce unwanted variability and bias into decisions, creating rampant injustices and high monetary costs even when the bias and variability go unnoticed.

Second, a small set of rules augmented by artificial intelligence can be more accurate than human judgment in making many decisions. As Kahneman noted, “[s]imple rules that are merely sensible typically do better than human judgment.”⁶⁵ Rules reduce the role of judgment and limit the number of factors

59. See generally Daryl Lim, *AI & IP: Innovation & Creativity in an Age of Accelerated Change*, 52 AKRON L. REV. 813 (2018).

60. Matthew Hutson, *Artificial Intelligence Prevails at Predicting Supreme Court Decisions*, SCIENCE (May 2, 2017), <https://www.sciencemag.org/news/2017/05/artificial-intelligence-prevails-predicting-supreme-court-decisions>.

61. See *infra* Part V.

62. See *infra* Part V. See, e.g., *QuikTrip W., Inc. v. Weigel Stores, Inc.*, 984 F.3d 1031, 1034 (Fed. Cir. 2021).

63. See KAHNEMAN ET AL., *supra* note 3, 337; see also KAHNEMAN ET AL., *supra* note 3, 336. (“A great deal of evidence suggests that algorithms can outperform human beings on whatever combination of criteria we select.”).

64. See *infra* Part V.

65. See KAHNEMAN ET AL., *supra* note 3, 133

to the most relevant ones—ones which AI can parse and offer more precise and readily examinable options to judges in helping them resolve disputes. This refined framework provides a transparent, easy-to-apply, and relatively cheap means of disposing cases during summary proceedings.

III. INSIDE TRADEMARK'S BLACK BOX: THE LIKELIHOOD OF CONFUSION

As trademark law's liability lynchpin, the LOC standard plays a critical role. Confusion likely exists between trademarks when they are so similar and the goods and/or services for which they are used are so related that consumers would mistakenly believe they come from the same source. The standard protects brand owners' investments and provides innovative signaling devices for consumers. When consumers can rely on a dependable commercial lexicon, they reward the owners, who gain an incentive to invest in quality products and service⁶⁶

Yet, like an untended garden, the LOC standard has grown wild. Different circuit courts have spun off anywhere between six and thirteen factors to ascertain the likelihood of confusion.⁶⁷ The standard needs a fresh rethinking to address the blended doctrines and new triggers for liability that have crept into it over the years.⁶⁸ A crisper, simplified framework brings the benefits of clarity—cheaper, more efficient dispute resolution, laws mapped to policy goals, better-calibrated doctrines in other areas of trademark law, and sharper boundaries between trademarks and other types of intellectual property rights.⁶⁹

Part A introduces the tremendous value of brand equity and the role of trademark law in safeguarding that equity. Unfortunately, it is difficult for anyone—courts, disputing parties, and the public—to determine when the law should intervene. Part B explains how the law became this way. Part C makes the case for clarity. Legal uncertainty has encouraged owners to vigorously assert trademarks, leading to an explosion of litigation. Unmeritorious claims redefine the public perception of trademark scope and ultimately shape those rights through a consumer perception feedback loop.

66. *Id.* at 1.

67. *See infra* Section III.B.

68. *See infra* Section III.B.

69. *See infra* Section III.C.

A. FROM BRAND EQUITY TO BABEL

Brands help businesses signal to consumers how the products and services they offer differ from their rivals.⁷⁰ Those brands may come to the public through words, logos, and package designs,⁷¹ infused with vivid metaphors and imagery and injected with mass media campaigns.⁷² Once sold as undifferentiated products, ketchup, coffee, and even water signal their desirability to consumers using brands like *Heinz*, *Starbucks*, and *Smartwater*.⁷³

Consumers rely on familiar brands to quickly navigate products or services that have attributes these businesses tout without having to physically inspect, experiment with, or consume each one.⁷⁴ Brands create mental anchors of goodwill and brand loyalty guides consumers toward existing or new products or services whose quality they have come to depend on.⁷⁵ The difference this branding confers to a product or service is known as brand equity.⁷⁶

Brand equity is worth a tremendous amount. In 2022, the overall value of the top 100 global brands reached over \$3 trillion, including the ubiquitous *Coca-Cola*, worth more than \$57 billion.⁷⁷ Unsurprisingly, developing brand equity also requires a business to invest heavily, sometimes millions of dollars.⁷⁸ A reliable commercial lexicon, in turn, encourages companies to invest in quality.⁷⁹ This virtuous cycle produces a competitive marketplace where consumers make informed purchases and companies invest in better products to accrue goodwill.⁸⁰ Unfortunately, brand equity also tempts some to free ride

70. Ronald C. Goodstein, Gary J. Bamossy, Basil G. Englis & Howard S. Hogan, *Using Trademarks as Keywords: Empirical Evidence of Confusion*, 105 TRADEMARK REP. 732, 734 (2015) (calling it “one of the most important concepts developed in marketing and the law”).

71. JANE C. GINSBURG, JESSICA LITMAN, & MARY L. KEVLIN, TRADEMARK AND UNFAIR COMPETITION LAW 17 (4th ed. 2007) (defining trademarks and their purpose).

72. Alex Kozinski, *Trademarks Unplugged*, 68 N.Y.U. L. Rev. 960, 973 (1993).

73. Kevin Lane Keller, *Conceptualizing, Measuring, and Managing Customer-Based Brand Equity*, 57 J. MKTG. 1, 1–22 (Jan. 1993).

74. Jacob Jacoby, *The Psychological Foundations of Trademark Law: Secondary Meaning, Genericism, Fame, Confusion and Dilution*, 91 TRADEMARK REP. 1013, 1014 (2001).

75. *See, e.g.*, *Qualitex Co. v. Jacobson Prods. Co.*, 514 U.S. 159, 163–64 (1995).

76. *See, e.g.*, Adam Hayes, *Brand Equity*, INVESTOPEDIA, (Feb. 22, 2021) <https://www.investopedia.com/terms/b/brandequity.asp> (“Brand equity refers to a value premium that a company generates from a product with a recognizable name when compared to a generic equivalent.”).

77. *Best Global Brands 2022*, INTERBRAND, <https://interbrand.com/best-brands/> (last visited Jan. 9, 2023); *see also* *DHL Corp. v. Comm’r*, 285 F.3d 1210, 1219 (9th Cir. 2002) (upholding a Tax Court valuation of DHL’s mark at \$100 million).

78. Keller, *supra* note 73, at 1–22.

79. Barton Beebe, *The Semiotic Analysis of Trademark Law*, 51 UCLA L. REV. 621, 623 (2004).

80. *Cf.* S. REP. NO. 79-1333, at 4 (1946); S. REP. NO. 79-1333, at 4 (1946).

on another business's accrued goodwill, misleading consumers into believing their inferior counterfeits embody the positive qualities of the business's original offerings.⁸¹ As a result, widespread counterfeiting mars consumers' view of the original product or service and hurts its sales.⁸² Trademark law guards against such harms.

Trademark law derives from common law antifraud doctrines.⁸³ Put simply, the law helps businesses and the public ensure that if consumers want Coke, they should not be served Pepsi or, worse, counterfeit Coke. In cyberspace, freeriding can take the form of search engines selling brands as a keyword to rivals to augment their standing by association with the famous mark at the expense of brand owners' sales and brand equity.⁸⁴ By safeguarding authenticity, trademark law helps keep clear the signals that brands send to consumers. Unfortunately, it is difficult for anyone—courts, disputing parties, and the public—to determine when the law should intervene to protect those signals.⁸⁵ Understanding how the law got to become this way is the first step to fixing it.

81. See, e.g., Joseph A. Belonax & Robert A. Mittelstaedt, *Evoked Set Size as a Function of Number of Choice Criteria and Information Variability*, in 5 ASS'N FOR CONSUMER RSCH., NA—ADVANCES IN CONSUMER RESEARCH 48 (Kent Hunt ed., 1978).

82. William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 J.L. & ECON. 265, 269–70 (1987).

83. BEVERLY W. PATTISHALL, DAVID C. HILLIARD & JOSEPH NYE WELCH II, TRADEMARKS AND UNFAIR COMPETITION § 1.02, at 4 (4th ed. 2000) (“Unfair competition is the genus of which trademark infringement is one of the species. Under this view, all trademark cases are in fact cases of unfair competition . . . and this is merely the duty to abstain from fraud.”).

84. Goodstein et al., *supra* note 71, at 735.

85. Beebe, *supra* note 21, at 1582 (pronouncing LOC standard “in a severe state of disrepair. Its current condition is Babelian”); Goodstein et al., *supra* note 71, at 1633 (“Basic concepts are no longer consistently applied and mistakes of doctrine are common.”); see also Stacey L. Dogan & Mark A. Lemley, *Grounding Trademark Law Through Trademark Use*, 92 IOWA L. REV. 1669, 1693 (2007) (agreeing that the law is “both substantively and procedurally ill-suited to resolve the complex set of issues raised by today’s novel trademark claims”); Michael Grynberg, *Things Are Worse Than We Think: Trademark Defenses in A “Formalist” Age*, 24 BERKELEY TECH. L.J. 897, 909 (2009) (noting that “the basic fact question of whether consumers are likely to be confused is a murky one”) [hereinafter Grynberg, *Things Are Worse*]; Michael Grynberg, *Trademark Litigation as Consumer Conflict*, 83 N.Y.U. L. REV. 60, 68 (2008) (describing LOC as “vulnerable to outcome-oriented manipulation”); Mark A. Lemley & Mark McKenna, *Irrelevant Confusion* 62 STAN. L. REV. 413 (2010) (failing to track consumer harm); Thomas R. Lee, Glenn Christensen & Eric DeRosia, *Trademarks, Consumer Psychology, and the Sophisticated Consumer*, 57 EMORY L.J. 575, 576 (2008) (describing LOC as “a vacuous war of words, uninformed by any careful theoretical modeling of consumer psychology or empirical study of consumer behavior”); Robert A. Kearney, *What Trademark Law Could Learn from Employment Law*, 12 J. MARSHALL REV. INTELL. PROP. L. 118, 129 (2012) (describing LOC as “a hopelessly, and maybe even ridiculously, directionless calculus”).

B. THE LANHAM ACT AND THE LIKELIHOOD OF CONFUSION

Through the Commerce Clause, Congress enacted the Trademark Act, colloquially called the Lanham Act (the “Act”) in 1946.⁸⁶ The Act codified common law doctrines but did not guide the application of the multifactor test to determine the likelihood of confusion.⁸⁷ In his treatise on trademark law, Thomas McCarthy observed that courts quickly gave trademark law “new and potent content” as they interpreted the statute.⁸⁸ As the fulcrum of trademark law, the entire infringement inquiry rests on courts determining the nature and scope of the LOC standard as appropriate for each new set of facts.

The Act protects registered and unregistered marks used in commerce by prohibiting free riders from using another’s word, name, symbol, or device in commerce in a way that is likely to confuse consumers.⁸⁹ Confusion may arise in various ways, most commonly when consumers mistake defendants’ products with plaintiffs’ products (“source confusion”). Other forms of confusion include thinking plaintiffs sponsor defendants’ products (“sponsorship confusion”) or that defendants and plaintiffs are affiliated (“affiliation confusion”).⁹⁰ Successful plaintiffs can enjoy injunctive relief, lost profits, costs of the action, and, in rare cases, attorneys’ fees.⁹¹ A well-functioning infringement system improves market efficiency,⁹² enables

86. See U.S. CONST. art. I, § 8, cl. 3; Lanham Act, 15 U.S.C. § 1114 (2016).

87. See Robert C. Denicola, *Some Thoughts on the Dynamics of Federal Trademark Legislation and the Trademark Dilution Act of 1995*, 59 L. & CONTEMP. PROBS., 75, 77–80 (1996) (“[T]he Lanham Act codifie[d] the basic common law principles governing both the subject matter and scope of [[trademark] protection.”).

88. J. Thomas McCarthy, *Lanham Act § 43(a): The Sleeping Giant is Now Wide Awake*, 59 L. & CONTEMP. PROBS. 45, 46 (1996).

89. § 1114 establishes a cause of action for registered marks (and therefore as the general trademark infringement statute) and § 1125 establishes a cause of action for unregistered marks (and therefore the statute for federal unfair competition). The Senate Committee on Patents described trademark law as, on the one hand, “protect[ing] the public so that it may be confident that, in purchasing a product . . . , it will get the product which it asks for and wants to get,” and, on the other hand, protecting a trademark owner’s expenditure of “energy, time, and money in presenting to the public the product . . . from . . . misappropriation by pirates and cheats.” S. Rep. No. 79-1333, at 3 (1946).

90. See MCCARTHY, *supra* note 13, §§ 23:1–4.

91. 15 U.S.C. §§ 1116–17, 1125(a).

92. Landes & Posner, *supra* note 83, at 265–66.

consumer choice,⁹³ safeguards free speech,⁹⁴ and disposes of claims efficiently.⁹⁵

This common law-style rulemaking has its advantages. Focusing on the parties and their peculiar issues allows judges to develop the law incrementally.⁹⁶ Unfortunately, fact-specificity also makes it hard to draw useful precedents to guide business compliance decisions and later interpretations by the courts.⁹⁷ Congress left operative terms like “likelihood” and “confusion” undefined.⁹⁸ This vacuum invites judges to weigh in.⁹⁹ Each of the thirteen circuits has its own formulation, employing between six and thirteen overlapping factors.¹⁰⁰ Some circuits favor factors that others ignore, and in different circumstances, lower courts have identified nearly every factor or factor combination as the most important.¹⁰¹ The reason for this may be divergent conceptions of trademark policy, with some courts focusing on unfair competition while others concentrate on consumer confusion.¹⁰² As a

93. See, e.g., Laura A. Heymann, *The Public’s Domain in Trademark Law: A First Amendment Theory of the Consumer*, 43 GA. L. REV. 651, 656 (2009) (arguing that “trademark law would benefit from incorporating a vision of the consumer rooted in a theory of autonomy.”).

94. See, e.g., Lisa P. Ramsey, *Descriptive Trademarks, and the First Amendment*, 70 TENN. L. REV. 1095, 1146 (2003) (explaining that descriptive terms used as marks are commercial speech “subject to an intermediate level of constitutional scrutiny under the Central Hudson test”).

95. See, e.g., Robert G. Bone, *Enforcement Costs and Trademark Puzzles*, 90 VA. L. REV. 2099, 2101 (2004) (discussing “the costs of enforcing trademark law, including the administrative costs of adjudicating trademark lawsuits and the error costs of over- and under-enforcing trademark rights”).

96. See, e.g., Oliver Wendell Holmes, *Codes, and the Arrangement of the Law*, 5 AM. L. REV. 1, 1 (1870).

97. See *Resorts of Pinehurst, Inc. v. Pinehurst Nat’l. Corp.*, 148 F.3d 417, 422 (4th Cir. 1998) (“The likelihood of confusion is a factual issue dependent on the circumstances of each case.”).

98. *GoTo.com, Inc. v. Walt Disney Co.*, 202 F.3d 1199, 1205 (9th Cir. 2000) (“The likelihood of confusion is the central element of trademark infringement.”); RESTATEMENT (THIRD) OF UNFAIR COMPETITION Ch. 3 § 20(1) (same); MCCARTHY, *supra* note 13, § 23:1 (“likelihood of confusion” is a fundamental test of trademark infringement); Barton Beebe & C. Scott Hemphill, *The Scope of Strong Marks: Should Trademark Law Protect the Strong More Than the Weak?*, 92 N.Y.U. L. REV. 1339, 1340 (2017) (describing the likelihood of confusion determination as the “central question in most trademark litigation”).

99. Graeme B. Dinwoodie, *Developing Defenses in Trademark Law*, 13 LEWIS & CLARK L. REV. 99, 137 (2009) (“[T]he basic theory of the Lanham Act allows greater common law development of defenses by courts.”).

100. MCCARTHY, *supra* note 13, § 24:30; see *Sally Beauty Co. v. Beautyco, Inc.*, 304 F.3d 964, 972 (10th Cir. 2002) (six factors); *In re E. I. Du Pont de Nemours & Co.*, 476 F.2d 1357, 1361 (C.C.P.A. 1973) (thirteen factors).

101. Beebe, *supra* note 21, at 1583.

102. Alejandro Mejías, *The Multifactor Test for Trademark Infringement from A European Perspective: A Path to Reform*, 54 IDEA 285, 314 (2014) (finding “there is also divergence on how the factors are treated and employed”); see Beebe, *supra* note 21, at 1591, 1596–97

result, courts in subsequent cases and businesses and their legal advisors struggle to determine the appropriate strength of each factor, either alone or relative to other factors.¹⁰³

To exacerbate things, circuits apply different standards of review to lower court LOC determinations. Some appeals courts review LOC under a “clearly erroneous” standard, with that deferential standard for factual inquires making it difficult to police errancy.¹⁰⁴ Others treat it as a question of law or a mixed question of law and fact,¹⁰⁵ perhaps to give themselves more latitude.

A few scholars have insisted that these LOC tests are uniform where they count.¹⁰⁶ To this view, Blake Tierney’s wry response is:

[t]he likelihood of confusion factors have remained substantially unchanged for nearly a century, not because they are the best possible answer to the question of when consumers are likely to be confused, but because each court simply does what the court before it did without much consideration for why the court before it did what it did.¹⁰⁷

(summarizing in chart form the different factors each circuit considers and reporting “substantial intercircuit variation in plaintiff multifactor test win rates”).

103. Joseph P. Liu, *Two-Factor Fair Use?*, 31 COLUM. J.L. & ARTS 571, 579 (2008) (“Under a multi-factor balancing test, it is difficult to register the relative strength of the factors.”); Eric Goldman, *Online Word of Mouth and its Implications for Trademark Law*, in TRADEMARK LAW AND THEORY: A HANDBOOK OF CONTEMPORARY RESEARCH 404, 424 (GRAEME B. DINWOODIE & MARK D. JANIS EDS., 2008) (“Assessing consumer confusion about product source is an inherently inexact process.”).

104. See *Arrow Fastener Co., Inc. v. Stanley Works*, 59 F.3d 384, 391 (2d Cir. 1995) (“We review the district court’s treatment of each *Polaroid* factor under a clearly erroneous standard. . . . Whether the plaintiff proved a likelihood of confusion is a legal question, and we review the court’s weighing of those factors and its ultimate conclusion under a de novo standard.”); see also Frederick Schauer, *Do Cases Make Bad Law?*, 73 U. CHI. L. REV. 883, 894 (2006).

105. 1 CHARLES MCKENNEY & GEORGE F. LONG III, FEDERAL UNFAIR COMPETITION: LANHAM ACT 43(a) § 12:3 (1989), UNFAIRCOMP § 3:8 (Westlaw database updated Apr. 2009); see, e.g., *Bristol-Myers Squibb Co. v. McNeil-P.P.C. Inc.*, 973 F.2d 1033, 1043 (2d Cir. 1992) (stating that the standard of review is de novo).

106. David J. McKinley, *Proving Likelihood of Confusion: Lanham Act vs. Restatement*, 12 J. CONTEMP. LEGAL ISSUES 239, 243 (2001) (“After a [brief] period of disparity, the lists developed by the various federal circuits have converged; differences from one list to another have become fairly minimal.”); see also Note, *Confusion in Cyberspace: Defending and Recalibrating the Initial Interest Confusion Doctrine*, 117 HARV. L. REV. 2387, 2392 n.27 (2004) (“Although the factors of this test vary from circuit to circuit, there is little substantive variation among the tests.”).

107. Blake Tierney, *Missing the Mark: The Mislplaced Reliance on Intent in Modern Trademark Law*, 19 TEX. INTELL. PROP. L.J. 229, 236 (2011).

Indeed, judges themselves admit the distinctions they make are often done on an “intuitive basis” rather than through “logical analysis.”¹⁰⁸

Empirical evidence backs Tierney’s view. Reporting on his dataset of cases, Beebe observed that “scattered among the circuits are factors that are clearly obsolete, redundant, or irrelevant, or, in the hands of an experienced judge or litigator, notoriously pliable.”¹⁰⁹ Based on the 331 cases he reviewed, the Second Circuit’s test in *Polaroid Corp. v. Polaroid Electronics Corp.* was the most frequently deployed test.¹¹⁰ In *Polaroid*, Judge Friendly articulated what became known as the eight *Polaroid* factors:

- (1) strength of the plaintiff’s mark;
- (2) similarity of plaintiff’s and defendant’s marks;
- (3) competitive proximity of the products;
- (4) likelihood that plaintiff will “bridge the gap” and offer a product like a defendant’s;
- (5) actual confusion between products;
- (6) good faith on the defendant’s part;
- (7) quality of defendant’s product; and
- (8) sophistication of the buyers.¹¹¹

Here, it is worth pausing to consider the fact that as an evidentiary standard, *colorable* instances of similarity that *likely* confuse may be all plaintiffs need to prove. Plaintiffs may succeed even if the marks are merely colorable and even if it is possible some consumers are not confused.¹¹² When defendants counterfeit the trademark outright, liability is clear.¹¹³ However, like patents and copyright, trademarks protect their owners beyond literal infringement.¹¹⁴ Nonliteral infringement exposes parties to uncomfortably

108. *Union Carbide Corp. v. Ever-Ready Inc.*, 531 F.2d 366, 379 (7th Cir. 1976).

109. Beebe, *supra* note 21, at 1583–84; *see also id.* at 1643 (“The factors relating to the similarity of the parties’ advertising, marketing, and sales facilities all tended to be redundant of the proximity of the goods factor in the circuits that consider these issues separately from the proximity factor.”)

110. *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492, 495 (2d Cir. 1961). Beebe, *supra* note 21, at 1593.

111. 287 F.2d at 495 .

112. *See, e.g.*, *Equitable Nat’l Life Ins. Co., Inc. v. AXA Equitable Life Ins. Co.*, 434 F. Supp. 3d 1227, 1249 (D. Utah 2020) (isolated, anecdotal instances insufficient).

113. *See, e.g.*, *UL LLC v. Space Chariot Inc.*, 250 F.Supp.3d 596 (2017).

114. *See generally*, Daryl Lim, *Judging Equivalents*, 36 SANTA CLARA HIGH TECH. L.J. 223 (2020).

uncertain waters.¹¹⁵ Patent law requires claims to give notice of their metes and bounds.¹¹⁶ Neither trademark nor copyright law has such claim requirements, leaving courts without statutory or judicial guidance on operationalizing technical similarity or market substitution considerations.¹¹⁷ Aside from the simplest forms of counterfeiting, the threshold for triggering confusion, and more so *likely* confusion, exists only as a relative measure where reasonable minds may differ, just as they do in the asylum and criminal cases discussed in Part II. Unlike real property, there are no metes and bounds. This lack of boundaries presents interpretive challenges due to LOC's current uncertainty.¹¹⁸

Lack of boundaries is common to other areas of the law. In any case, though, the LOC standard's indeterminacy muddies not just trademark law's focal point but also trademark rights as a whole, as well as adjacent disciplines like copyright and patent law.¹¹⁹ That indeterminacy also acts as a drag on dispute resolution, compliance, and social equity. The rational response must be to clarify the law.

115. See Michael Grynberg, *Thick Marks, Thin Marks*, 67 CASE W. RES. L. REV. 13, 15 (2016) (“Many open questions in modern trademark law concern which parts of the range belong under the trademark holder’s control.”).

116. 35 U.S.C. § 112(b) (requiring patentees to include in their patent “one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor . . . regards as the invention”).

117. See Jeanne C. Fromer & Mark A. Lemley, *The Audience in Intellectual Property Infringement*, 112 MICH. L. REV. 1251, 1296–99 (2014) (analyzing how trademark law emphasizes market substitution over technical similarity standards).

118. Michael Grynberg, *The Judicial Role in Trademark Law*, 52 B.C. L. REV. 1283, 1303 (2011) (“Trademark’s fundamental inquiry, whether a likelihood of confusion exists, invites judicial lawmaking in no small part because the term ‘likelihood of confusion’ presents an interpretive problem.”); Graeme W. Austin, *Tolerating Confusion About Confusion: Trademark Policies and Fair Use*, 50 ARIZ. L. REV. 157, 160 (2008) (“[There is] considerable uncertainty about some of the key questions that are germane to the factual inquiry at the heart of the likelihood of confusion analysis.”); see also generally Daryl Lim, *Saving Substantial Similarity*, 73 FLA. L. REV. 591, 601–02 (2021) (discussing the challenges of vagueness and uncertainty of nonliteral infringement in the copyright context); *id.* at 593 (“Judges and scholars have called the court-developed tests to assess substantial similarity ‘ad hoc,’ ‘bizarre,’ and ‘a virtual black hole in copyright jurisprudence.’”).

119. See, e.g., Robert G. Bone, *Notice Failure and Defenses in Trademark Law*, 96 B.U. L. REV. 1245, 1255 (2016) (“[W]hat makes the scope of rights so uncertain is the vagueness of the likelihood-of-confusion test (‘LOC test’) for infringement.”); Amy Adler & Jeanne C. Fromer, *Taking Intellectual Property into Their Own Hands*, 107 CALIF. L. REV. 1455, 1523 (2019) (“Trademark law is similarly complex and unpredictable with regard to important doctrines.”).

C. THE CASE FOR CLARITY

Overprotection could cause a chilling effect on marketplace competition if even compliant businesses face the specter of trademark litigation from overzealous owners. Ascertaining whether consumers might see a connection between an owner and alleged infringement is a complicated business. William McGeeveran warned that ascertaining liability before the litigation is “impossible.”¹²⁰ That indeterminacy may not be a bad thing. When liability is difficult to predict, risk-averse users tend to obtain a license even if not needed since there is currently no cheap and easy way to test confusion claims.¹²¹ As unsavory as it might be for licensees, trademark law does not prohibit that outcome. Trademark owners have the right to control how they and others use their marks. It is easier for them to assess whether their mark has spillovers (positive or negative) in deciding whether to license.¹²² Besides adapting to new situations, the uncertainty may nudge potential licensees into self-identifying, seeking licenses from owners, facilitating an efficient exchange of market value.¹²³

As in the real world, the danger with this tactic is the systemic risk of overfishing, or overenforcement. Brand managers and their trademark attorneys have every incentive to do so. Both base their professional success on strengthening brand equity.¹²⁴ In her work on online agreements, Leah Chan-Grinvald’s research reported that “[t]rademark holders are under the misapprehension that every third-party use of a trademark must be stopped, or else their trademarks will not be considered strong.”¹²⁵ Likewise, empirical work by William Gallagher suggests trademark owners routinely

120. William McGeeveran, *Four Free Speech Goals for Trademark Law*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1205, 1214–15 (2008) (“[I]t may be impossible to anticipate in advance how confusing a judge will find your client’s parody of, or allusion to, a trademark.”).

121. David S. Welkowitz, *The Virtues and Vices of Clarity in Trademark Law*, 81 TENN. L. REV. 145, 146 (2013) (“[T]rademark owner threatens litigation, an early outcome is relatively unlikely, and even cases decided before trial may prove expensive.”).

122. See Bone, *supra* note 95, at 2100–01 (discussing the negative costs of enforcing trademark law and trademark lawsuits); see also Kenneth L. Port, *Trademark Extortion: The End of Trademark Law*, 65 WASH. & LEE L. REV. 585 (2008) (discussing how trademark holders sue competitors to secure market share).

123. See, e.g., James Gibson, *Risk Aversion and Rights Accretion in Intellectual Property Law*, 116 YALE L.J. 882, 913 (2007) (“It should therefore come as no surprise when trademark users who could mount a decent defense against infringement claim nevertheless choose to seek a license.”).

124. See, e.g., *Procter & Gamble Co. v. Johnson & Johnson Inc.*, 485 F. Supp. 1185, 1207 (S.D.N.Y. 1979) (“[T]rademark law not only encourages but requires one to be vigilant on pain of losing exclusive rights.”).

125. Leah Chan Grinvald, *Contracting Trademark Fame?*, 47 LOY. U. CHI. L.J. 1291, 1309 (2016).

“overenforce” trademark rights when they know their claims are weak—i.e., the likelihood of confusion is extremely low. Lawyers who Gallagher interviewed shared it was appropriate and even expected that they had “an asserted ethical duty to zealously advocate client interests were readily invoked to justify aggressive policing of IP rights.”¹²⁶

These sentiments, coupled with the enormous value of trademarks, may explain why trademark litigation has exploded over the past few decades.¹²⁷ Owners threaten lawsuits and resist early dismissals, even when the offending use furthers First Amendment or other ostensibly laudable interests, instead cowing potential infringers into licensing agreements rather than engaging in costly litigation conflicts.¹²⁸ Median costs of trademark suits that get through the discovery phase (and also through trial) vary between \$150,000 through discovery (\$300,000 through trial) on the low end, and up to \$750,000 through discovery (\$1.5 million through trial) on the high end.¹²⁹ Defendants waiting until trial to weed out frivolous claims face \$300,000–\$1.25 million in legal fees alone.¹³⁰ Such expensive and time-consuming disputes may involve inquiries into defendants’ intent, and requests for survey evidence underpinned by expensive dueling experts.¹³¹ Allowing settlements in the shadow of a vague LOC standard caters to an attitude that assumes confusion is illegal and likely protected by law. Moreover, most potential defendants simply want to avoid liability cleanly and efficiently, capitulating rather than challenging the merits of suits against them.¹³² As a result, rivals, particularly risk-averse small or medium businesses, may choose not to advertise or invest in their developing brands once subject to a trademark litigation dispute.

Unmeritorious claims redefine the public perception of trademark scope and ultimately shape those rights through a consumer perception feedback

126. William T. Gallagher, *Trademark and Copyright Enforcement in the Shadow of IP Law*, 28 SANTA CLARA HIGH TECH. L.J. 453, 496–97 (2012).

127. *See id.*

128. Welkowitz, *supra* note 122, at 152 (“[A] potential defendant may forego expressive activity rather than risking a lawsuit.”). *Cf.* Randy J. Kozel & David Rosenberg, *Solving the Nuisance-Value Settlement Problem: Mandatory Summary Judgment*, 90 VA. L. REV. 1849, 1855–58 (2004) (describing the problem of civil plaintiffs filing meritless suits, and the economics and strategy behind a defendant’s decision to settle such suits).

129. *See* AM. INTELL. PROP. LAW ASS’N, REPORT OF THE ECONOMIC SURVEY 35 (2013).

130. *See* AM. INTELL. PROP. LAW ASS’N, REPORT OF THE ECONOMIC SURVEY 22 (2005).

131. *Indianapolis Colts, Inc. v. Metro. Balt. Football Club Ltd. P’ship*, 34 F.3d 410, 414–16 (7th Cir. 1994) (Posner, J.) (discussing expert reports presented by both sides in a trademark dispute).

132. McGeeveran, *supra* note 121, at 1214.

loop.¹³³ Imagine a world where grocery stores must separate similar products to avoid any risk of association. In that world, companies could take licenses rather than pay to litigate. Over time, it would become rarer to see similar products grouped. Soon, even a can of generic cola beside Coke would confuse consumers. In such a world, if a grocer put a generic cola and Coke together in an aisle, the grocer would risk liability for freeriding Coke's interest in being insulated from rivals by selling generic colas.¹³⁴

Chan-Grinvald's research on online agreements indicates the problem of unmeritorious claims is also pernicious on the internet. Trademark owners assert an unprecedented number of keyword-based trademark threats against the media, book publishers, movie and television creators, search engines, comparative advertisers, critics, and parodists.¹³⁵ For example, digital platforms help aggregate product reviews for easy price and quality comparisons.¹³⁶ To do this, website operators need to use others' trademarks to communicate effectively with consumers. Unfortunately, brand owners have attempted to shut down those uses based on affiliation or source confusion in court.¹³⁷

The Supreme Court warned in *Wal-Mart Stores, Inc. v. Samara Bros* of plaintiffs using indeterminacy in trademark law to overreach and bully defendants into submission, and thus chill legitimate activities.¹³⁸ Yet, the law's current approach to the LOC standard breeds precisely the kind of behavior the Court warned against—allowing bullying by trademark owners and forcing defendants to litigate to clarify their rights.¹³⁹ This is an unfair and dangerous way for the legal system to ensure compliance, and it has not gone unnoticed. Stacey Dogan warned that “markets could not function without some means for sellers to determine whether their marketing plans might infringe someone else's trademark. This requires the ability of individuals or companies interested in creating their own trademark to identify other protected marks

133. Mark P. McKenna, *Trademark Use and the Problem of Source*, 2009 U. ILL. L. REV. 773, 774 & n.4 (2009) (“Consumer expectations largely define trademark rights, yet those expectations are influenced by consumers' understanding (or misunderstanding) of the law.”).

134. Dogan & Lemley, *supra* note 86, at 1694–95.

135. Dogan & Lemley, *supra* note 86, at 1695 (reporting thousands of keyword-based trademark threats every year).

136. *See, e.g., Toyota Motor Sales, U.S.A., Inc. v. Tabari*, 610 F.3d 1171 (9th Cir. 2010) (trademark defendants ran website compiling automobile dealer pricing and providing matching services).

137. *See id.* at 1175 (“Toyota is using this trademark lawsuit to make it more difficult for consumers to use the Tabaris to buy a Lexus.”).

138. *Wal-Mart Stores, Inc. v. Samara Bros., Inc.*, 529 U.S. 205, 214 (2000) (finding that “[c]ompetition is deterred . . . not merely by successful suit but by the plausible threat of successful suit”).

139. I am grateful to Jon Lee for this insight.

and to have some confidence about the scope of existing-trademark protection.”¹⁴⁰ In this regard, trademark law “fall[s] well short of the mark.”¹⁴¹ If the government expects businesses to abide by the law, then the law needs to be clear and predictable.¹⁴²

The bottom line is that the LOC standard needs to be clearer about what it expects from judges and litigants. A well-functioning standard helps set expectations for judges and litigants, creates stability and minimizes litigation costs, increases the speed of judicial decision-making, and benefits other trademark law. As the court in *Samara Bros* observed, “[h]ow easy it is to mount a plausible suit depends, of course, upon the clarity of the test.”¹⁴³ The status quo prejudices consumers, individuals, and fledgling brands who are not repeat players. Ordinary users for purposes of art or commentary typically lack expertise about trademark law and the resources to obtain legal advice.¹⁴⁴ Furthermore, critical to any property system, including trademark rights, is proper notice about the existence and scope of those legal rights to the public. Poor notice adds to litigation costs for potential victims of trademark bullying, increases information costs by directing users to more costly search strategies,¹⁴⁵ impedes efficient licensing, and ultimately discourages innovation.¹⁴⁶ A patchwork of inconsistent results destabilizes the system for everyone, even plaintiffs.¹⁴⁷ Beyond litigation, uncertainty over the confusion standard leads parties to assign different estimates to the value of a license. It

140. Stacey Dogan, *Bullying and Opportunism in Trademark and Right-of-Publicity Law*, 96 B.U. L. REV. 1293, 1297–98 (2016).

141. *Id.*

142. Kenneth A. Matuszewski, *Casting Out Confusion: How Exclusive Appellate Jurisdiction in the Federal Circuit Would Clarify Trademark Law*, 18 W. MICH. U. COOLEY J. PRAC. & CLINICAL L. 31, 43 (2016) (“Because the test is not uniform, practitioners trying to interpret the Act and precedent will only end up confused.”).

143. *Wal-Mart Stores, Inc.* 529 U.S. at 213.

144. Users may be consumers or fledgling brands and are “litigants” for the purposes of this argument. See Boris Shapiro, *Note, Trademark Arbitration: A First Rate Change for a Second Life Future*, 8 J. INTELL. PROP. 273, 287 (2009) (“While in-game users may have a legitimate belief that their business practices do not infringe real world trademarks, they must nevertheless factor the costs of litigation into the equation. Furthermore, faced with uncertainties such as the length of a trial, the amount of discovery required, the success of winning on the merits and the likelihood of appeal, the in-game business owner may feel defeated before stepping into the court-house. Notwithstanding the strength of his case, he will feel powerless in the face of an opponent with potentially unlimited time and resources”).

145. See Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 580-81 (1992) (discussing the incentives to seek legal advice under rules and standards).

146. See Bone, *supra* note 119, at 1257.

147. Thomas H. Watson, *Pay Per Click: Keyword Advertising and the Search for Limitations of Online Trademark Infringement Liability*, 2 CASE W. RESERVE J.L. TECH. & INTERNET 101, 122 (2011).

causes negotiations to break down, harming *both* brand owners and potential licensees.¹⁴⁸

Conversely, expedient determinations, which can only occur when the law is clear, serve the ends of justice for both sides. Summary judgments provide a quick and inexpensive exit ramp for parties to dispose of a case when no real issues call for a trial. The ability of courts to wield this important judicial tool protects defendants against frivolous lawsuits and plaintiffs from incurring unnecessary costs.¹⁴⁹ Streamlining the test by consolidating and trimming down the factors will enable courts to get to the heart of the inquiry expeditiously. Clarifying the LOC standard lowers the temperature and makes it easier for owners to determine when to protect their interests. Part VI shows how.

Simplifying confusion will benefit other aspects of trademark law. For example, trademark law's first sale doctrine lets others sell used or reconditioned goods with the original mark, which also incorporate confusion.¹⁵⁰ Nominative fair use may likewise fold LOC into its analysis.¹⁵¹ What is "fair" implicates the confusion arising from the trademark's use, whether the defendant only used as much as necessary of the plaintiff's mark, which in turn infects the plaintiff's mark with the vagueness of the LOC standard.¹⁵² The same issue arises with the use of expressive trademarks¹⁵³ or the keyword advertising.¹⁵⁴

148. See Bone, *supra* note 119, at 1258.

149. Elaine Kussurelis, *Canada's Summary Trial Procedure: A Viable Alternative to Summary Judgment on Trademark Likelihood of Confusion Actions in the United States*, 50 U. MIAMI INTER-AM. L. REV. 165, 168 (2019) (observing summary judgments "can be a powerful trademark litigation weapon for either plaintiffs or defendants").

150. The first sale doctrine states that a trademark owner cannot prevent someone who has lawfully purchased a trademarked good from selling that item to someone else. This allows the distribution of trademarked goods beyond the initial sale by the trademark owner. See *Nitro Leisure Prods., L.L.C. v. Acushnet Co.*, 341 F.3d 1356, 1362–64 (Fed. Cir. 2003) (consumer confusion as benchmark for applying the first sale doctrine).

151. *Toyota Motor Sales, U.S.A., Inc. v. Tabari*, 610 F.3d 1175–76 (9th Cir. 2010) (determining normative fair use occurs by asking whether (1) the product was readily identifiable without use of the mark; (2) defendant used more of the mark than necessary; or (3) defendant falsely suggested he was sponsored or endorsed by the trademark holder).

152. E.g., *KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc.*, 543 U.S. 111, 123 (2004) (discussing if confusion relevant to whether descriptive use is "fair").

153. See *Rogers v. Grimaldi*, 875 F.2d 994, 999 (2d Cir. 1989) (adopting balancing test that asks whether the use of a trademark as the title of an expressive work is artistically relevant to the underlying work and, if so, whether "the title explicitly misleads as to the source or the content of the work").

154. See *Network Automation, Inc. v. Advanced Sys. Concepts, Inc.*, 638 F.3d 1137, 1154 (9th Cir. 2011) (holding that use of mark in keyword advertising is not likely to cause confusion).

Likewise, potential infringers may be liable for dilution. Dilution occurs when defendants either tarnish the plaintiff's mark with unsavory associations or when they blur its distinctiveness with multiple uses on different products.¹⁵⁵ It does not require plaintiffs to show a likelihood of confusion.¹⁵⁶ While liability for dilution is theoretically distinct from confusion, it frequently tracks similar facts when courts consider a mark's fame and the subjective "blurring" of marks in the public mind.¹⁵⁷ Defining the hard edges of the LOC standard will allow courts to develop trademark law more coherently and transparently.

Clarity also helps police the boundaries beyond trademark law on the one hand and patent law and copyright law on the other.¹⁵⁸ Trademarks, unlike patents and copyright, last indefinitely and could give a trademark owner monopoly power without the threshold requirements and other limitations that patent and copyright law demand of their respective rights holders.¹⁵⁹

The risk of overextending trademark rights is particularly true in product design cases where trade dress adjoins both copyright and patent rights.¹⁶⁰ For instance, clothing makers can obtain trademark protection for signature features of the clothing,¹⁶¹ while original textile designs can receive copyright protection for the pattern on clothing.¹⁶² Questions have also arisen over whether the design of a sign supported on the bottom by two springs constituted protectable trade dress,¹⁶³ whether VIP's "Bad Spaniels Silly Squeaker" dog toy, which was roughly the same shape as a bottle of Jack Daniel's but with "dog-related twists" was "aesthetically functional,"¹⁶⁴ or

155. *See, e.g.*, 15 U.S.C. §§ 1125(c)(2)(A)–(B) (2012) (listing factors for determining whether a mark is famous and whether the defendant's use dilutes by blurring). *See* Bone, *supra* note 120; Robert G. Bone, *Hunting Goodwill: A History of the Concept of Goodwill in Trademark Law*, 86 B.U. L. REV. 547, 604-06 (2006) (identifying the link between LOC and dilution).

156. *See, e.g.*, *Moseley v. V Secret Catalogue, Inc.*, 537 U.S. 418, 432–33 (2003) (clarifying the basis of dilution claims in trademark law).

157. William McGeveran, *Rethinking Trademark Fair Use*, 94 IOWA L. REV. 49, 70 (2008).

158. *See, e.g.*, *Qualitex Co. v. Jacobson Prods. Co.*, 514 U.S. 159, 164 ("It is the province of patent law, not trademark law, to encourage invention by granting inventors a monopoly over new product designs or functions for a limited time.").

159. *See* Landes & Posner, *supra* note 83, at 287 ("The lack of a fixed term for trademarks is one of the striking differences between trademarks, on the one hand, and copyrights and patents, on the other."); *see generally* 15 U.S.C. § 1114 (remedies for trademark infringement).

160. *See, e.g.*, *Star Athletica, L.L.C. v. Varsity Brands, Inc.*, 580 U.S. 405354 (2017) (copyright eligibility of useful article design at issue).

161. *See generally* 15 U.S.C. § 1051 (trademark registration application requirements).

162. *See* COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 924.3(A)(1) (3d ed. 2014).

163. *Traffix Devices, Inc. v. Marketing Displays, Inc.* 532 U.S. 23, 24 (2001).

164. *VIP Prods. LLC v. Jack Daniel's Prods., Inc.*, 953 F.3d 1170, 1172 (9th Cir. 2020).

whether a thin, partially chocolate-dipped biscuit cookie was utilitarian.¹⁶⁵ Understanding where to mark the doctrinal cloth between the disputed marks requires appreciating how the standard for confusion itself became confusing.

IV. ROOTS OF CONFUSION

Over the years, the jurisprudential roots of trademark law became unruly and tangled. Unfair competition intermingled with consumer protection as the Lanham Act blended trade names and technical trademarks.¹⁶⁶ A later legislative revision untied the LOC standard from source confusion—a different part of the trademark infringement analysis. When interpreting the revision, courts then introduced idiosyncratic rules of affiliation and sponsorship as triggers for consumer confusion.¹⁶⁷ Within the LOC tests, factors such as defendants' intent, survey evidence, and consumer sophistication provided a convenient but misguided attempt to determine trademark infringement.¹⁶⁸ Judges resorted to coherence-based reasoning, finding the satisfaction of other factors once they were satisfied that their favored factors were present.¹⁶⁹ It made their work easier but muddied the waters for everyone else.

A. EXPANSION INTO CONFUSION

1. *Blending the Law on Trade Names and Trademarks*

The scope of trademark law historically protects virtually anything that functions as a source identifier—shapes, colors, smells, and sounds.¹⁷⁰ Today, the law goes even further. As a result of the 1988 amendment to the Lanham Act, trademark law now covered new types of protectable subject matter, from technical trademarks to almost anything capable of carrying source meaning, as potential trademarks.¹⁷¹ As a result, the LOC standard became more complex. This Section explains the origins of these developments and their implications.

165. *Ezaki Glico Kabushiki Kaisha v. Lotte Int'l Am. Corp.*, 986 F.3d 250, 253 (3d Cir. 2021), as amended (Mar. 10, 2021).

166. *See infra* Section IV.A.

167. *See Toyota Motor Sales, U.S.A., Inc. v. Tabari*, 610 F.3d at 1175 (“Toyota is using this trademark lawsuit to make it more difficult for consumers to use the Tabaris to buy a Lexus.”).

168. *See infra* Section IV.C.

169. *See infra* Section IV.D.

170. *See Bone, supra* note 120, at 1268.

171. *Qualitex Co. v. Jacobson Prods. Co.*, 514 U.S. 159, at 162.

At its origin, trademark common law in the late nineteenth century distinguished between trade names and technical trademarks.¹⁷² Most trade name disputes involved rivals.¹⁷³ Unfair competition law governed these disputes and focused on directly competing uses that diverted trade,¹⁷⁴ taking the form of passing off or reverse passing off business names.¹⁷⁵

Defendants who used their first or last names as trade names reasonably expected they could do so, even if those names happened to be like the plaintiffs' names.¹⁷⁶ Instead of comparing trade names in a dispute, courts required plaintiffs to prove the defendants' intent to confuse or mislead the public as well as proof of actual harm.¹⁷⁷ Even when plaintiffs succeeded, they only obtained narrow injunctions so defendants could continue to operate their business.¹⁷⁸

Unlike trade names that could be descriptive, technical trademarks had to be fanciful, arbitrary, or suggestive.¹⁷⁹ The 1905 Trade-Mark Act mapped infringement to unauthorized use, which held "substantially the same descriptive properties as those set forth in [plaintiff's] registration."¹⁸⁰ The infringement threshold was lower because plaintiffs had only to prove consumers would be confused without proving intent or actual confusion.¹⁸¹ And unlike with trade names, infringement of technical trademarks was based

172. See FRANK I. SCHECHTER, *THE HISTORICAL FOUNDATIONS OF THE LAW RELATING TO TRADE-MARKS* 161 (1925).

173. Edward S. Rogers, *The Lanham Act and the Social Function of Trademarks*, 14 L. & CONTEMP. PROB. 173, 178–80 (1949).

174. See Mark P. McKenna, *The Normative Foundations of Trademark Law*, 82 NOTRE DAME L. REV. 1839, 1904 (2007) (noting that courts only developed the likelihood of confusion factors after jettisoning the requirement of direct competition).

175. "Passing off" occurs when defendants sell their goods with the plaintiff's mark, with "reverse passing off," defendants sell plaintiff's goods with the defendant's trademark, see Corporate Counsel's Guide to Unfair Competition § 25:1 (2012).

176. MCCARTHY, *supra* note 13, § 4:5.

177. See SCHECHTER, *supra* note 172.

178. See, e.g., *Kellogg Co. v. Nat'l Biscuit Co.*, 305 U.S. 111, 122 (1938) ("Sharing in the goodwill of an article unprotected by patent or trade-mark is the exercise of a right possessed by all—and in the free exercise of which the consuming public is deeply interested. There is no evidence of passing off or deception on the part of the Kellogg Company; and it has taken every reasonable precaution to prevent confusion or the practice of deception in the sale of its product.").

179. See *Canal Co. v. Clark*, 80 U.S. 311, 323 (1871).

180. Trade-Mark Act of 1905, Pub. L. No. 58–84, § 16, 33 Stat. 724, 728, repealed by Lanham Act, Pub. L. No. 79–459, § 46(a), 60 Stat. 427, 444 (1946) (codified as amended in various sections of 15 U.S.C.).

181. See SCHECHTER, *supra* note 172, at 161.

on a strict liability standard.¹⁸² Finally, compared with trade name cases, courts in technical trademark cases routinely granted blanket injunctions, regardless of whether doing so would put the defendant out of business.¹⁸³

In the twentieth century, courts blurred the distinction between the two. As sellers expanded into adjacent product markets in the post-war era, courts expanded the scope of protection to include complementary products and services.¹⁸⁴ For instance, a trademark for pancake syrup infringed another for pancake batter.¹⁸⁵ The Act also codified the blended standard, requiring only that the unauthorized use be connected with goods or services.¹⁸⁶ Trade names enjoyed the protection offered to technical trademarks as long as owners could show “secondary meaning.”¹⁸⁷ Cases interpreted this as customers associating the source of the product that imbued trade names with an acquired distinctiveness.¹⁸⁸ The Act subsequently welded the two concepts, allowing all kinds of signs to acquire distinctiveness through secondary meaning.¹⁸⁹

Table 1: Trade Names, Technical Trademarks and Modern Trademark

	Trade Names	Technical Trademarks	Modern Trademarks
Distinctiveness	Sufficient if descriptive	Requires distinctiveness	Sufficient if descriptive
Intent	Intent required	Strict Liability	Intent optional
Harm	Actual harm required	Likelihood of harm sufficient	Likelihood of harm sufficient
Comparison	No	Yes	Optional
Injunction	Narrow	Broad	Broad

182. A trade name is generally considered the name a business uses for advertising and sales purposes, *see* MCCARTHY, *supra* note 13, § 30:1.

183. Milton Handler & Charles Pickett, *Trade-Marks and Trade Names—An Analysis and Synthesis*, 30 COLUM. L. REV. 168, 169 (1930).

184. *See* PAMELA WALKER LAIRD, ADVERTISING PROGRESS: AMERICAN BUSINESS AND THE RISE OF CONSUMER MARKETING 31 (1998) (discussing post-war expansion of consumer products).

185. *Aunt Jemima Mills Co. v. Rigney & Co.* 247 F. 407 (2d Cir. 1917).

186. *See* Lanham Act § 32(1)(a) (2016).

187. *See, e.g.*, Handler & Pickett, *supra* note 183, at 200.

188. *See* *E. Columbia, Inc. v. Waldman*, 181 P.2d 865 (Cal. 1947).

189. *Compare* 15 U.S.C. § 1052(f) (2006), *with* Trade-Mark Act of 1905, Pub. L. No. 58–84, § 5(b), 33 Stat. 724, 725–26.

Table 1 shows how the modern trademark standard blended the most expansive aspects of the previous standards in favor of the trademark owner such as likelihood of harm rather than actual harm or broad injunction rather than a narrow one. Law and economics scholarship, driven by a belief that stronger protection maximized wealth and, in turn, promoted economic efficiency, prompted this expansion.¹⁹⁰ The result infused unfair competition into trademark law and invited courts to find defendants' marks infringing well before consumers make a purchase, based on the idea that defendants misappropriated the plaintiff's goodwill to appeal to consumers.¹⁹¹

In practical terms, the fused standard gave businesses using descriptive terms like "fish fry"¹⁹² the same broad injunctive relief previously reserved for distinctive trademarks. In policy terms, trademark law, once consumer-centered, was in effect displaced by brand equity.¹⁹³ Scholars like Rochelle Dreyfuss, Mark Lemley, and Mark McKenna expressed alarm at this shift and its implications for trademark doctrine.¹⁹⁴ Trademark law contains no rule protecting brand equity even where there is no evidence that defendants caused harm.¹⁹⁵ Yet, that is precisely what aggressive owners have attempted, as they claim functional subject matter,¹⁹⁶ block comparative advertising by rivals,¹⁹⁷ and harass rivals.¹⁹⁸ Today, the law does not require plaintiffs to define that goodwill and show misappropriation.¹⁹⁹ Instead, courts use likely consumer confusion as a proxy to determine the boundaries of protectable goodwill.

190. See Landes & Posner, *supra* note 83, at 270–79, (advancing Chicago School economic theory within trademark law's scope); see, e.g., *W. T. Rogers Co. v. Keene*, 778 F.2d 334, 339 (7th Cir. 1985) (Posner J.) (finding that "competition is not impaired by giving each manufacturer a perpetual 'monopoly' of his identifying mark" if the manufacturer has chosen a "distinctive" trademark where the available names are "for all practical purposes infinite").

191. *Gibson Guitar Corp. v. Paul Reed Smith Guitars*, 423 F.3d 539, 549 (6th Cir. 2005).

192. *Zatarains, Inc. v. Oak Grove Smokehouse, Inc.*, 698 F.2d 786, 788 (5th Cir. 1983).

193. Barton Beebe, *Search and Persuasion in Trademark Law*, 103 MICH. L. REV. 2020, 2072 (2005). ("The consumer, once sovereign, has been deposed, deprivileged, decentered.")

194. See Rochelle Cooper Dreyfuss, *Expressive Genericity: Trademarks as Language in the Pepsi Generation*, 65 NOTRE DAME L. REV. 397, 399 (1990) ("[T]he changing legal climate has tended to grant trademark owners greater control over their marks."); Lemley & McKenna, *supra* note 86, at 414 (arguing that "trademark law needs to refocus on confusion that is actually relevant to purchasing decisions").

195. Beebe & Hemphill, *supra* note 99, at 1390–91.

196. See, e.g., *TraFFix Devices, Inc. v. Mktg. Displays, Inc.*, 532 U.S. 23, 23–24 (2000).

197. See, e.g., *Toyota Motor Sales, U.S.A., Inc. v. Tabari*, 610 F.3d, at 1180.

198. See, e.g., *Ga.-Pac. Consumer Prods., LP v. Myers Supply, Inc.*, 621 F.3d 771, 775–77 (8th Cir. 2010); *Ga. Pac. Consumer Prods., LP v. Von Drehle Corp.*, 618 F.3d 441, 442 (4th Cir. 2010).

199. See Bone, *supra* note 119, at 569–72 (reviewing the different attempts to define the term "goodwill" and noting that goodwill escapes precise definition).

Scholars disagree whether trademark expansionism has resulted in a net positive and whether trademark rights should be narrower or broader.²⁰⁰ This Article takes no stand on that normative debate but instead breaks ground on another one, arguing that the fusion is a key contributing factor to muddying the LOC standard.

2. *Yet More Triggers for Confusion*

When Congress amended the Act in 1962, it removed the restriction that confusion was limited to source confusion.²⁰¹ Courts thereafter dutifully expanded the scope of confusion from purchasers to include non-purchasers (“post-sale confusion”) and allowed businesses to prohibit confusion over sponsorship or endorsement of goods and services.²⁰² Whereas protection previously stopped at the shores of adjacent products, trademark law expanded to allow even a pancake chain restaurant to attempt to prohibit an evangelical organization from using a similar mark.²⁰³ This caused a jurisprudential disjuncture to occur.

Factors like consumer sophistication, the likelihood of expansion, and marketing channels have told us nothing about evaluating a brand company’s claim to be the exclusive soda associated in the minds of consumers with a sporting event.²⁰⁴ Worse, the multiple factors that the LOC standard now targets make applying the standard even more unwieldy and unpredictable.²⁰⁵

Trademark litigation is inherently impressionistic, particularly when actual confusion is rare. Courts caught up in the swirl sloppily peppered their judgments with different operative terms to describe the same thing, including

200. See Bone, *supra* note 119, at 1268.

201. See S. Rep. No. 87-2107, at 4 (1962) reprinted in 1962 U.S.C.C.A.N. 2844, 2847. Act of Oct. 9, 1962, Pub. L. No. 87-772 § 2, 76 Stat. 769, 769 (deleting the requirement that confusion be of “purchasers as to the source of origin of such goods or services”).

202. Act of Oct. 9, 1962, Pub. L. No. 87-772 § 2, 76 Stat. 769, 769 (deleting the requirement that confusion be of “purchasers as to the source of origin of such goods or services”). See, e.g., *New Kids on the Block v. News Am. Publ'g, Inc.*, 971 F.2d 302, 309 (9th Cir. 1992) (recognizing sponsorship or endorsement as relevant in determining normative fair use in trademark infringement analysis).

203. See generally Demand for Jury Trial, *IHOP IP, LLC v. Int’l House of Prayer*, No. CV10-6622-SHO-SHX, 2010 WL 3775268 (C.D. Cal. Sept. 9, 2010).

204. Supreme Assembly, *Order of Rainbow for Girls v. J.H. Ray Jewelry Co.*, 676 F.2d 1079, 1082 (5th Cir. 1982) (“other association”); *Caterpillar Inc. v. Walt Disney Co.*, 287 F. Supp. 2d 913, 918 (C.D. Ill. 2003) (“otherwise affiliated”).

205. Gibson, *supra* note 124, at 908 (“The case law on sponsorship and approval, however, is so ambiguous as to make it almost impossible to know ex ante whether a given use will be infringing.”).

“affiliation,”²⁰⁶ “endorsement,”²⁰⁷ “connection,”²⁰⁸ to whether the use produced confusion “of any kind.”²⁰⁹ As the Fifth Circuit bluntly put it, “Congress adopted an open-ended concept of confusion. Any kind of confusion will now support an action for trademark infringement.”²¹⁰

Substitution bias is particularly virulent when open-ended wording gives courts cover, as the Act did here.²¹¹ Courts took that opportunity and leaned into LOC factors like defendants’ intent, survey evidence, and trademark strength, which were malleable and easy to wield to reach their desired outcomes.²¹² Strikingly, Beebe’s empirical study reported that intent and surveys were so heavily weighted that courts stamped over other factors.²¹³ Unfortunately, if LOC outcomes turn on evidence of intent and survey evidence, then trademark infringement is fundamentally flawed. The next two Sections explain why.

B. AN INTENT TO CONFUSE

Judges may like for there to be evidence of intent because it makes their jobs easier, and the outcome feel just. All circuits but the Federal Circuit recognize this as a major factor in finding liability.²¹⁴ However, eliminating intent allows a judge to focus their inquiry into the likelihood of confusing a trademark rather than the commercial immorality of defendants. Intent should be removed as a factor for determining the likelihood of confusion. This is because it is based on the defendant rather than the consumer. and with little relevance to a consumer’s perception of a mark or potential for confusion, and muddies jurisprudential waters.²¹⁵

The LOC standard’s intent factor examines whether defendants sought to benefit from plaintiffs’ goodwill.²¹⁶ Once plaintiffs show that defendants know

206. *E.g.*, *Pebble Beach Co. v. Tour 18 I Ltd.*, 155 F.3d 526, 544 (5th Cir. 1998).

207. *Id.*

208. *SNA, Inc. v. Array*, 51 F. Supp. 2d 554, 562–63 (E.D. Pa. 1999) (concluding that defendants’ attempt to use metatags to “lure internet users to their site” was in bad faith), *aff’d sub nom.*

209. *Syntex Labs., Inc. v. Norwich Pharmacal Co.*, 437 F.2d 566, 568 (2d Cir. 1971).

210. *Armstrong Cork Co. v. World Carpets, Inc.*, 597 F.2d 496, 501 n.6 (5th Cir. 1979).

211. *See, e.g., SNA, Inc.* 51 F. Supp. 2d at 562–63.

212. *See supra* Section III.C.

213. Beebe, *supra* note 21, at 1607.

214. *See* Beebe, *supra* note 21, at 1589–90.

215. For an example of specific circuit language that currently use “intent” as a factor, *see, e.g., Stone Creek, Inc. v. Omnia Italian Design, Inc.*, 875 F.3d 426, 434 (9th Cir. 2017) (“Omnia’s reason for adopting the STONE CREEK mark also plays a critical role: when the alleged infringer intended to deceive customers, we infer that its conscious attempt to confuse did in fact result in confusion.”)

216. *Sicilia Di R. Beibow & Co. v. Cox*, 732 F.2d 417, 431 (5th Cir. 1984).

about plaintiffs' marks, courts assume intent.²¹⁷ The Restatement on Unfair Competition notes that courts may then infer confusion from wrongful intent since "it may be appropriate to assume that an actor who intends to cause confusion will be successful in doing so."²¹⁸ To see how this causal inference works, consider the Second Circuit's reasoning that defendants intended to capitalize on the Steinway trademark by adopting the "Steinweg" name and slogan even though consumers would not mistake a Grotrian-Steinweg piano for a Steinway piano at the time of purchase.²¹⁹ The court explained that "the harm to Steinway . . . is the likelihood that a consumer, hearing the 'Grotrian-Steinweg' name and thinking it has some connection with 'Steinway,' would consider it on that basis."²²⁰ Beverly Pattishall suggested that whether or not a defendant intends to confuse consumers makes outcomes more predictable.²²¹ It seems then that if a defendant intends to confuse consumers, a court will more likely find there to be a likelihood of confusion because it may be easier to determine the state of mind of one person, the defendant, than to forecast the perceptions of the consumer group.

Predictability is good, but the result may not be, as anyone having indulged in a night of merriment and subsequently endured a hangover will attest. Defendants' intent plays an outsized influence because it is an easy proxy for courts to weigh the equities of the case rather than the underlying factual inquiry.²²² Courts look at defendants' intent to copy a mark rather than confuse the public,²²³ switching between "intent to confuse" and "intent to copy" interchangeably.²²⁴

Intent inherently focuses on the wrong goalpost. Merely because the defendant's mental state is easier to discern than the consuming public does not make that factor more relevant to the inquiry. As Kelly Collins warned,

217. *Maker's Mark Distillery, Inc. v. Diageo N. Am., Inc.*, 679 F.3d 410, 424 (6th Cir. 2012).

218. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 22 cmt. B (1995). *AMF Inc. v. Sleekcraft Boats*, 599 F.2d 341, 354 (9th Cir. 1979) ("[T]he defendant can accomplish his purpose: that is, that the public will be deceived.").

219. See *Grotrian, Helfferich, Schulz, Th. Steinweg Nachf. v. Steinway & Sons*, 523 F.2d 1331, 1342 (2d Cir. 1975).

220. See *id.*

221. See Beverly W. Pattishall, *The Impact of Intent in Trade Identity Cases*, 60 TMR 575, 579–80 (1970).

222. See, e.g., MCCARTHY, *supra* note 13, § 23:110 ("[C]ourts sometimes engage in the traditional rhetoric that accompanies punishing the evildoer.").

223. See *A & H Sportswear, Inc. v. Victoria's Secret Stores, Inc.*, 237 F.3d 198, 225–26 (3d Cir. 2000).

224. E.g., *Nautilus Group, Inc. v. ICON Health & Fitness, Inc.*, 372 F.3d 1330, 1336–37 (Fed. Cir. 2004) (using "intent to confuse" and "intent to copy" interchangeably within the same paragraph).

“[t]his is dangerous because mere ‘copying’ is not always impermissible.”²²⁵ The law encourages reusing generic or functional marks “as a part of our competitive economic system.”²²⁶ For this reason, she argues that the relevant intent is intent to confuse and not merely to copy.²²⁷

David Tan and Benjamin Foo agree with Collins, observing that intent is “controversial as it has little or no bearing on consumers in the marketplace.”²²⁸ Grynberg warned that intent “lacks a necessary nexus to existence of likelihood of confusion,” making it “open to manipulation by the factfinder.”²²⁹ Moreover, “[t]he elusive nature of the underlying inquiry similarly invites appellate overreaching.”²³⁰ Alejandro Mejías explained that intent is irrelevant because the focus “is not what the defendant intended to do, but whether his mark is likely to be confusingly similar for the relevant public.”²³¹ Very few courts have acknowledged as much.²³²

There is another reason to ditch intent—it muddies jurisprudential waters caused by the fusion of trade name and technical trademark jurisprudence further. Courts require intent when dealing with non-inherently distinctive marks.²³³ For inherently distinctive marks, courts have either presumed intent or dispensed with it.²³⁴ Technical trademark infringement focuses on the consequences of the defendant’s act and not on their intent.²³⁵ In contrast,

225. Kelly Collins, *Intending to Confuse: Why Preponderance Is the Proper Burden of Proof for Intentional Trademark Infringements Under the Lanham Act*, 67 OKLA. L. REV. 73, 87 (2014).

226. *Id.*

227. *Id.* at 87-88 (“This would better serve the purposes of the Lanham Act and safeguard innocent conduct from triggering liability.”).

228. David Tan & Benjamin Foo, *The Extraneous Factors Rule in Trademark Law: Avoiding Confusion or Simply Confusing?*, 2016 SING. J. LEGAL STUD. 118, 133 (2016). Thomas L. Casagrande, *A Verdict for Your Thoughts? Why an Accused Trademark Infringer’s Intent Has No Place in Likelihood of Confusion Analysis*, 101 TRADEMARK REP. 1447, 1455 (2011) (“[E]vidence of wrongful intent is not helpful to the underlying empirical inquiry, namely, whether consumer confusion is likely.”).

229. Grynberg, *Things Are Worse*, *supra* note 85, at 910.

230. Grynberg, *Things Are Worse*, *supra* note 86, at 910 n.57.

231. Mejías, *supra* note 103, at 349.

232. *See, e.g.*, *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 151 (2d Cir. 2003) (Intent is not “of high relevance to the issue of likelihood of confusion. . . . It does not bear directly on whether consumers are likely to be confused.”).

233. MCCARTHY, *supra* note 13, § 23:105.

234. *See* *Cashmere & Camel Hair Mfrs. Inst. v. Saks Fifth Ave.*, 284 F.3d 302, 317 (1st Cir. 2002); *Res. Developers, Inc. v. Statue of Liberty-Ellis Island Found., Inc.*, 926 F.2d 134, 140 (2d Cir. 1991).

235. Margreth Barrett, *Finding Trademark Use: The Historical Foundation for Limiting Infringement Liability to Uses “In the Manner of A Mark”*, 43 WAKE FOREST L. REV. 893, 909 (2008) (Noting as to intent that “plaintiffs in secondary meaning infringement cases generally

trade name infringement focuses on defendants' desired outcomes, irrespective of consumer confusion.²³⁶ The modern standard melds both, making it an unstable and dangerous factor.

The Act does not require proof of intent. Trademark law is, after all, a strict liability offense.²³⁷ As the Sixth Circuit opined, the better view is to consider intent only after other LOC factors indicate liability.²³⁸ Intent may go to aggravated remedies but should be irrelevant to the question of guilt. As Beebe put it, "if trademark law seeks to prevent commercial immorality, then it should do so explicitly. An injunction should issue, and damages be granted on that basis alone, and not based on possibly distorted findings of fact as to the likelihood of consumer confusion."²³⁹

The final reason may be surprising given the seeming outsized role intent plays according to conventional wisdom. Beebe's data revealed that intent was of decisive importance in the few cases where they featured.²⁴⁰ In other words, intent is doctrinally irrelevant and, when looking at case law in the aggregate, empirically irrelevant as well.

Judges may like intent because it makes their job easier, and the outcome feels just. However, intent is irrelevant to technical trademark infringement. Eliminating intent allows a more focused inquiry into LOC rather than the commercial immorality of defendants. As a practical matter, it frees parties from costly discovery and allows the court to grant summary judgment more frequently, producing the benefits discussed in Section IVC.²⁴¹ Judges can

had to demonstrate that the defendant acted with fraudulent intent, while courts would presume fraud in technical trademark infringement cases.")

236. *See, e.g.,* *Shaver v. Heller & Merz Co.*, 108 F. 821, 827 (8th Cir. 1901) ("Everyone has the right to use and enjoy the rays of the sun, but no one may lawfully focus them to burn his neighbor's house Everyone has the right to use pen, ink, and paper, but no one may apply them to the purpose of defrauding his neighbor of his property, or making counterfeit money, or of committing forgery.")

237. *See* *Taubman Co. v. Webfeats*, 319 F.3d 770, 775 (6th Cir. 2003) (recognizing that the Lanham Act is a "strict liability statute"); *see also* Rebecca Tushnet, *Running the Gamut From A to B: Federal Trademark and Federal False Advertising Law*, 159 U. PA. L. REV. 1305, 1310 (2011) (noting that federal courts have interpreted trademark as a strict liability offense); Bone, *supra* note 95, at 2109 (referring to trademark infringement as a form of strict liability).

238. *See, e.g.,* *Taubman Co.*, 319 F.3d at 775 ("[T]he proper inquiry is not one of intent. In that sense, the Lanham Act is a strict liability statute. If consumers are confused by an infringing mark, the offender's motives are largely irrelevant.")

239. Beebe, *supra* note 21, at 1631.

240. *Id.* at 1622.

241. 10B CHARLES ALAN WRIGHT, ARTHUR R. MILLER & MARY KAY KANE, FEDERAL PRACTICE AND PROCEDURE (CIVIL) § 2730 (3d ed. 1998) ("Questions of intent, which involve intangible factors including witness credibility, are matters for the consideration of the fact finder after a full trial and are not for resolution by summary judgment.")

dispose of cases more easily without trial and defendants will less likely be subject to vexatious suits based on the nebulous aspersions of intent.²⁴² The audience of trademark law are consumers, but even there, problematic proxies have infiltrated the LOC factors to trip judges up.

C. TRADEMARK'S AUDIENCE

While the “ordinary consumer” is central to the infringement analysis, he or she remains poorly theorized.²⁴³ In patent cases, courts benefit from expert testimony.²⁴⁴ Trademark law makes do with survey evidence of market substitution along with an assortment of policy goals. Judges must determine confusion without evidence that any consumers were confused, imagining consumers’ likely experience as filtered through their hypothetical competing interests. This notional consumer is “neither savant nor dolt,”²⁴⁵ but rather one who “lacks special competency with reference to the matter at hand but has and exercises a normal measure of the layman’s common sense and judgment.”²⁴⁶

The key problem here is bias—considering evidence that is irrelevant except for one’s personal biases. Like the rest of us, judges have subjective biases that consumers in the relevant marketplace may not share.²⁴⁷ This is particularly important when significant demographic differences separate the judge and average consumer. Courts are divided on the matter. In *Triangle Publications v. Rohrllich*, involved whether teenage girls would likely confuse SEVENTEEN in magazines for MISS SEVENTEEN used in girdles.²⁴⁸ On appeal, the dissenting judge criticized the trial judge’s “shaky kind of guess” that the ordinary female teenage consumer was likely confused by the two marks.²⁴⁹ He argued that the right approach was to survey adolescent girls, their mothers, and their sisters.²⁵⁰

242. Casagrande, *supra* note 228 (proposing an elimination of intent as a factor to be considered in determining trademark infringement).

243. See, e.g., Lee et al., *supra* note 85, at 575 (“[N]either courts nor commentators have made any serious attempt to develop a framework for understanding the conditions that may affect the attention that can be expected to be given to a particular purchase.”).

244. Douglas G. Smith, *The Increasing Use of Challenges to Expert Evidence Under Daubert and Rule 702 in Patent Litigation*, 22 J. INTELL. PROP. L. 345, 354 (2015).

245. Kraft Foods Grp. Brands LLC v. Cracker Barrel Old Country Store, Inc., 735 F.3d 735, 743 (7th Cir. 2013).

246. United States v. 88 Cases, More or Less, Containing Bireley’s Orange Beverage, 187 F.2d 967, 971 (3d Cir. 1951).

247. Kussurelis, *supra* note 149, at 174 (arguing that “judges plac[e] undue emphasis on facts taken out of the actual marketplace context.”).

248. DINWOODIE & JANIS, *supra* note 103, at 525.

249. *Triangle Publications v. Rohrllich*, 167 F. 2d 969, 976 (2d Cir. 1948).

250. *Id.* at 977.

Courts rely on surveys to determine trademark strength and consumer sophistication, and thus to answer the LOC question. Surveys are a form of evidence, while trademark strength and consumer sophistication are legal determinations. All of these inform the same inquiry—is there a likelihood of confusion? Like intent, none provide a good proxy. The Sections below explain why.

1. *Surveys are Expensive and Misleading*

In theory, parties attempt to use surveys in trademark disputes to measure whether consumers believe that the plaintiff's mark is the source of the alleged infringer's product or whether it sponsors or approves of the related product. In practice, courts routinely attack the representativeness of the survey from a parade of cherry-picked witnesses and extrapolate a standard of what consumers generally believe.

Surveys allow courts to determine how consumers responded to defendants' use of their mark.²⁵¹ Beebe touts surveys as “one of the most classic and most persuasive and most informative forms of trial evidence that trademark lawyers utilize in both prosecuting and defending against trademark claims of various sorts,”²⁵² reporting that courts draw negative inferences if plaintiffs fail to conduct surveys.²⁵³

Plaintiffs may provide survey evidence that an appreciable number of relevant consumers are likely to be confused.²⁵⁴ These surveys present consumers with defendants' marks and measure their reaction in the context consumers would encounter the mark in question.²⁵⁵ They typically involve control groups to show causality between the defendants' mark and consumer confusion.²⁵⁶ A survey needs to pass muster under the Federal Rules of Evidence, which requires considering the “validity of the techniques employed.”²⁵⁷ Courts can bar significantly flawed surveys as evidence when they are more prejudicial than probative²⁵⁸ or deemed unreliable.²⁵⁹

251. See MCCARTHY, *supra* note 13, § 23:17 (discussing survey evidence).

252. Beebe, *supra* note 21, at 1641.

253. See, e.g., *Eagle Snacks, Inc. v. Nabisco Brands, Inc.*, 625 F. Supp. 571, 583 (D.N.J. 1985).

254. See MCCARTHY, *supra* note 13, § 32:158.

255. Shari Seidman Diamond & David J. Franklyn, *Trademark Surveys: An Undulating Path*, 92 TEX. L. REV. 2029, 2037 (2014).

256. See, e.g., *Bracco Diagnostics, Inc. v. Amersham Health, Inc.*, 627 F. Supp. 2d 384, 448 (D.N.J. 2009) (criticizing a survey's design for failure to use “an adequate control mechanism”).

257. FED. JUD. CTR., REFERENCE MANUAL ON SCI. EVIDENCE 233–34 (2d ed. 2002).

258. *Citizens Fin. Group, Inc. v. Citizens Nat'l Bank*, 383 F.3d 110, 118–21 (3d Cir. 2004).

259. *Id.*

Given the perceived centrality of surveys, it is surprising that empirical studies reveal courts rely on survey evidence infrequently. Beebe's study revealed that only twenty percent of cases discussed survey evidence, and only ten percent were credited.²⁶⁰ It is just as well.

One reason that cases mention survey evidence so infrequently is that surveys are costly,²⁶¹ time-consuming, and even well-constructed ones are frequently challenged.²⁶² As Robert Bone explained, "surveys are difficult to design properly and expensive to conduct . . . Judges also find it difficult to evaluate survey methodology, especially when confronted with competing expert testimony, and this increases the likelihood of error."²⁶³ Identifying an expert to conduct surveys in the time available before a preliminary injunction hearing and the cost of doing so presents formidable challenges.²⁶⁴ Most parties also settle before trial.²⁶⁵

As a matter of justice between the parties, the staggering costs of surveys put defendants at a disadvantage. Bone explained that "[p]roving a high LOC puts a premium on surveys and expert testimony and is likely to require extensive discovery, all of which will increase direct litigation costs and strengthen a trademark owner's ability to leverage cease-and-desist threats in frivolous and weak cases."²⁶⁶

Bone is right to be concerned that surveys may be methodologically dicey. Rebecca Tushnet described the problem of verbal overshadowing in the

260. Beebe, *supra* note 21, at 1641 (only sixty-five (20%) of the 331 opinions discussed survey evidence and thirty-four (10%) credited the survey evidence.); Katie Brown, Natasha Brison & Paul Batista, *An Empirical Examination of Consumer Survey Use in Trademark Litigation*, 39 LOY. L.A. ENT. L. REV. 237, 244 (2019) ("Although survey evidence plays a critical role in trademark litigation, many disagree on the weight afforded by courts, or if it is actually a necessity.").

261. Robert H. Thornburg, *Trademark Surveys: Development of Computer-Based Survey Methods*, 4 J. MARSHALL REV. INTELL. PROP. L. 91, 91 (2004) (explaining that traditional trademark surveys have "prices ranging in the hundreds of thousands of dollars" and "are all subject to being discredited and devalued" due to procedural flaws).

262. Brown, *supra* note 260, at 245 ("[T]here is a pressing need for continuous research on consumer survey use in trademark litigation in order to establish additional evidence and to better develop consensus among the methodologies used.").

263. Bone, *supra* note 95, at 2131.

264. See MCCARTHY, *supra* note 13, § 32:196 (observing that "accurate and scientifically precise surveys" are not always introduced because they are costly, and litigants are better off not using a survey than using a survey "obtained on the cheap").

265. Beebe, *supra* note 21, at 1642 ("It may be objected that trademark litigation is typically resolved at the preliminary injunction stage before either party has had the time or can be expected to conduct a creditable survey. . . . [I]t is still striking that survey evidence played a relatively minor role even in the bench trial context.").

266. Bone, *supra* note 120, at 1269 n.110.

context of trademark surveys and noting that “questions themselves may change a respondent’s answers by changing the way she thinks. Being asked to give reasons distorts reasoning, especially when the question has little meaning for the respondent Once an idea has been brought to a respondent’s attention, he often thinks it relevant.”²⁶⁷

Consider *Anheuser-Busch, Inc. v. Balducci Publications*, where the court found infringement based on evidence that over half of those surveyed thought the defendant should have permission from the plaintiff to advertise, even though only six percent of consumers were confused by the disputed trademark.²⁶⁸ To the court, the plaintiff’s survey expert tweaked the questions to elicit spurious evidence of confusion.²⁶⁹ This low bar foments the idea that most consumers are dummies unable to distinguish between goods and services.

Another problem is that surveys attempting to capture sponsorship or endorsement confusion rely on broad and indeterminate operative terms that exacerbate the indeterminacy of the LOC standard.²⁷⁰ The most egregious among these terms is “permission”—when survey respondents opine on whether they think the owners need to give “permission” for the challenged use, they problematically convert consumer impression of licensing culture into law.²⁷¹ This word is misleading. Consumer beliefs may not map to policy imperatives and put the cart before the horse. Public perception about the legality of unlicensed trademark uses should be shaped by the law rather than defined by such uses.²⁷²

In theory, surveys attempt to measure whether consumers believe that the plaintiff’s mark is the source of the alleged infringer’s product or whether it sponsors or approves of that product.²⁷³ In practice, courts routinely attack the

267. Rebecca Tushnet, *Gone in Sixty Milliseconds: Trademark Law and Cognitive Science*, 86 TEX. L. REV. 507, 544–45 (2008).

268. 28 F.3d 769, 772–78 (8th Cir. 1994).

269. *Id.* at 775.

270. *See, e.g.*, *Processed Plastic Co. v. Warner Commc’ns, Inc.*, 675 F.2d 852, 854–55 (7th Cir. 1982) (“At the hearing, Warner Bros. introduced a survey of children between the ages of 6 to 12 in which 82% of the children identified a toy car identical to PPC’s Maverick Rebel as the “Dukes of Hazzard” car and of that number 56% of them believed it was sponsored or authorized by the “Dukes of Hazzard” television program.”).

271. Gibson, *supra* note 124, at 911 (“Courts’ reliance on such surveys to define the reach of the trademark entitlement thus amounts to a tautological endorsement of whatever consumers believe the law is, or should be, regardless of whether their beliefs make any sense from a policy standpoint.”).

272. Gibson, *supra* note 124, at 911 (“If that perception is formed at least in part by exposure to licensing practices, then the law conflates premise and conclusion and invites doctrinal feedback.”).

273. 3 ANNE GILSON LALONDE, GILSON ON TRADEMARKS § 8.03 (2021).

representativeness of the survey from a parade of cherry-picked witnesses and extrapolate a standard of what consumers generally believe.²⁷⁴ Judicial unease with surveys sometimes bubbles to the surface, with Judge Posner remarking once that “no doubt there are other tricks of the survey researcher’s black arts that we have missed.”²⁷⁵

There is a certain circular irony to the whole exercise. Courts rely on surveys only to support conclusions that they reach using other factors. The analysis also works backward—faced with survey evidence showing a likelihood of confusion, judges may regard the marks as more similar than they might have appeared in the absence of the survey.²⁷⁶ As Peter Weiss remarked, “one might sum it all up by saying that the function of surveys in trademark litigation is to plumb the minds of the public in order to make up the minds of the judges.”²⁷⁷ Dispensing of surveys and relying on the court’s judgment would not just be cheaper and simpler, it would also be the intellectually honest thing to do.

2. *Trademark Strength is Not the Answer*

A related issue is trademark strength. Surveys sometimes overlap with trademark strength since parties may use the former to measure the potency of a mark’s goodwill and its worthiness of protection.²⁷⁸ Known as the *Abercrombie* spectrum, generic and descriptive marks are not distinctive, suggestive marks are marginally distinctive, and arbitrary or fanciful are inherently distinctive.²⁷⁹ Trademark strength is usually the first factor courts consider.²⁸⁰

274. *Id.*

275. *Indianapolis Colts, Inc. v. Metro. Balt. Football Club Ltd. P’ship*, 34 F.3d at 416.

276. *Diamond & Franklyn*, *supra* note 255, at 2043.

276. *Diamond & Franklyn*, *supra* note 255, at 2043.

277. Peter Weiss, *The Use of Survey Evidence in Trademark Litigation: Science, Art or Confidence Game?*, 80 TRADEMARK REP. 71, 86 (1990).

278. Beebe, *supra* note 21, at 1646 (“In trademark law, the question is always of consumer perception in the marketplace rather than judicial perception in the courtroom.”).

279. *See Abercrombie & Fitch Co. v. Hunting World, Inc.*, 537 F.2d 4, 9 (2d Cir. 1976) (Identifying “four different categories of terms with respect to trademark protection. Arrayed in an ascending order which roughly reflects their eligibility to trademark status and the degree of protection accorded, these classes are (1) generic, (2) descriptive, (3) suggestive, and (4) arbitrary or fanciful.”).

280. *See, e.g., Welding Servs., Inc. v. Forman*, 509 F.3d 1351, 1361 (11th Cir. 2007) (“The stronger or more distinctive a trademark or service mark, the greater the likelihood of confusion.”). Beebe & Hemphill, *supra* note 99, at 1349 (“Strength is the first factor in the Second, Fourth, Fifth, Sixth, Eighth, Ninth, and Eleventh Circuits, the second factor in the Third Circuit, and the last factor in the First and Tenth Circuits.”). Courts consider design marks under the *Seabrook* factors. *See Seabrook Foods, Inc. v. Bar-Well Foods, Ltd.*, 568 F. 2d.

Strong trademarks are distinctive. Determining what the owner owns requires more than just looking at the mark; it requires assessing what protection the trademark owner should be entitled to for that mark.²⁸¹ Distinctive marks are memorable to consumers as to source indicators and possess greater conceptual strength.²⁸² Courts equate distinctiveness with a greater breadth of protection, are more willing to find confusing similarities,²⁸³ and that the strongest marks merit the widest range of protection.²⁸⁴

One court acknowledged distinctiveness “is far from an exact science and that the differences between the classes, which is not always readily apparent, makes placing a mark in its proper context and attaching to it one of the [*Abercrombie*] labels a tricky business at best.”²⁸⁵ Empirical studies confirm courts judge mark strength intuitively and erroneously.²⁸⁶ For instance, Beebe reported how courts failed to categorize the plaintiff’s mark in a specific category of distinctiveness in half of the cases he studied.²⁸⁷ He observed that “considerations such as the comparative quality of the parties’ goods or the inherent distinctiveness of the plaintiff’s mark rarely aid in this inquiry.”²⁸⁸

As a LOC factor, it is flawed. Scholars warn against assuming that judges can accurately gauge public perception.²⁸⁹ Lisa Ouellette observed that “[t]he

1342, 1344 (C.C.P.A. 1977) (“In determining whether a design is arbitrary or distinctive this court has looked to whether it was a ‘common’ basic shape or design, whether it was unique or unusual in a particular field, whether it was a mere refinement of a commonly-adopted and well-known form of ornamentation for a particular class of goods viewed by the public as a dress or ornamentation for the goods, or whether it was capable of creating a commercial impression distinct from the accompanying words.”).

281. *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 148 (2d Cir. 2003).

282. *See id.*

283. *See, e.g., First Sav. Bank, F.S.B. v. First Bank Sys., Inc.*, 101 F.3d 645, 655 (10th Cir. 1996) (“When the primary term is weakly protected to begin with, minor alterations may effectively negate any confusing similarity between the two marks.”).

284. *See, e.g., Ford Motor Co. v. Money Makers Auto. Surplus, Inc.*, No. 8:03CV493, 2005 WL 2464715, at *1, *3 (D. Neb. Sept. 14, 2005) (finding that the various Ford Motor Company marks at issue “are among the most famous marks in the world” and are “therefore entitled to the widest scope of protection”).

285. *Banff, Ltd. v. Federated Dep’t Stores, Inc.*, 841 F.2d 486, 489 (2d Cir. 1988).

286. *See, e.g., Beebe, supra* note 21, at 1633 (“The data suggest that, at least in the context of the multifactor test, the doctrine of trademark strength has broken down. Basic concepts are no longer consistently applied and mistakes of doctrine are common.”).

287. Beebe, *supra* note 21, at 1633–35 (stating that some use of the spectrum was made in only 193 out of 331 cases and that the mark was placed in a specific category in only 164 cases).

288. Beebe, *supra* note 21, at 1645.

289. Lisa Larrimore Ouellette, *The Google Shortcut to Trademark Law*, 102 CALIF. L. REV. 351, 362 (2014) (“there is little reason to expect that individual judges are particularly good at gauging public perception of a mark, especially given the significant demographic differences between the average judge and the relevant population of consumers in most cases.”).

complex doctrine that has evolved around trademark strength and the likelihood of confusion appears to be a (largely unsuccessful) attempt to provide some analytical rigor to the essential questions of how strongly a mark identifies goods or services and how well it distinguishes those products from others in the marketplace.”²⁹⁰ Others have variously criticized trademark strength as “needlessly open-ended.”²⁹¹

Mark strength does not correlate positively with whether marks deserve stronger protection. Stronger marks suffer from more free-riding only to a certain extent, which may not affect investment. For instance, free-riders using SUPER BOWL does not dampen the NFL’s investment in promoting and producing the event. Moreover, while it is true that more free-riding lowers the threshold of confusion, that does not mean more free-riding leads to more consumer confusion. As with survey evidence, McCarthy notes, that:

[A] cynic would say that . . . when the court wants to find no infringement, it says that the average buyer is cautious and careful . . . [b]ut if the judge thinks there is infringement, the judge sets the standard lower and says the average buyer is gullible and not so discerning.²⁹²

There is no requirement for LOC to consider either survey evidence or mark strength. Eliminating both would both simplify LOC and make it less prone to error.

3. *Consumer Sophistication is not the Answer*

Determining consumer sophistication provides the court with context of the consumer information available and the ability of consumers to discern between the marks.²⁹³ Vaunted as a decisive factor, the Fourth Circuit declared that it “virtually eliminating the likelihood of consumer confusion in the case of a professional or highly sophisticated buyer.”²⁹⁴ Courts consider the “consumer’s degree of care” in determining whether they would likely be confused.²⁹⁵ Sophisticated consumers resist impulse purchases but rather do

290. *Id.* at 360.

291. Timothy Denny Greene & Jeff Wilkerson, *Understanding Trademark Strength* (2013) 16 STAN. TECH. L. REV. 535 at 582.

292. MCCARTHY, *supra* note 13, § 23:92; *see also* Ann Bartow, *Likelihood of Confusion*, 41 SAN DIEGO L. REV. 717, 747 (2004).

293. Andrew Martineau, *Imagined Consumers: How Judicial Assumptions About the American Consumer Impact Trademark Rights, for Better and for Worse*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 337, 352 (2012) (“This would seem to be a crucial part of the test, given that the standard for infringement is whether consumers are likely to be confused.”).

294. Lee et al., *supra* note 86, at 581.

295. *E.g.*, *Sally Beauty Co. v. Beautyco, Inc.*, 304 F.3d 964, 975 (10th Cir. 2002).

so after what the First Circuit called “a careful consideration of the reliability and dependability of the manufacturer and seller of the product.”²⁹⁶ For this reason, all LOC tests consider whether consumers within the relevant market are sophisticated and careful.²⁹⁷

In their search and purchase decisions, courts seek to determine consumers’ care, using a reasonably prudent purchaser as to the baseline and adjusting for situations where consumers are less likely to be confused.²⁹⁸ For example, factors that may affect consumer care in transactions include whether the consumers have expertise in the field, the cost and complexity of the purchase, the length of the transaction timeline, the frequency of the purchase, as well as the education, age, gender, and income of the consumer.²⁹⁹

Scholars criticized the artificiality of consumer sophistication, likening it to expecting judges to perform a “Vulcan mind meld” with consumers in the marketplace.³⁰⁰ Consumer sophistication begs the question of how a judge would distinguish between those who are sophisticated and those who are unthinking and credulous. Courts may easily project their normative view of how carefully a consumer should be or its view of a defendant’s conduct.³⁰¹ Like intent, surveys, and mark strength, consumer sophistication suffers from inherent capriciousness.

There is plenty, but there is one final culprit. The sheer multitude of factors courts must consider also makes LOC difficult to deploy, bogging down courts to apply factors selectively. To cope, they rely on coherence-based reasoning to make sense of their findings.

D. ADDRESSING COHERENCE-BASED REASONING

This Section explains how decision-makers may consider a finite amount of information to reach a good enough approximation of “correct” outcomes. Their focus gravitates toward the most familiar or concrete factors while marginalizing less-familiar factors or those more difficult to ascertain. As a result, courts may weigh LOC factors impressionistically.

296. *Astra Pharm. Prods., Inc. v. Beckman Instruments, Inc.*, 718 F.2d 1201, 1206 (1st Cir. 1983).

297. MCCARTHY, *supra* note 13, §§ 24:30–43.

298. *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 151 (2d Cir. 2003).

299. *See AMF Inc. v. Sleekcraft Boats*, 599 F.2d 341, 353 (9th Cir. 1979).

300. *See William E. Gallagher & Ronald C. Goodstein, Inference Versus Speculation in Trademark Infringement Litigation: Abandoning the Fiction of the Vulcan Mind Meld* 94 TRADEMARK REP 1229, 1230 (2004).

301. *August Storck K.G. v. Nabisco, Inc.*, 59 F.3d 616, 618 (7th Cir. 1995) (“Many consumers are ignorant or inattentive, so some are bound to misunderstand no matter how careful a producer is.”).

Over the past century, trademark law ossified determining the LOC standard from a pragmatic judge-made rule of thumb into a rigid and formalistic standard.³⁰² The Restatement (First) merely mentioned “the following factors are important,”³⁰³ and the early cases applied the factors loosely.³⁰⁴ However, appeals courts slapped lower courts for failing to address each factor, with orders to reverse and remand.³⁰⁵ We can deduce that this formalism ended up burdening courts with an unwieldy craft, forcing judges to pay lip service to all the factors while systemically relying on only a few.³⁰⁶ At the same time, their opinions recite disclaimers that the LOC factors are only a guide and that no single factor is dispositive.³⁰⁷

Given their marching orders, one might expect judges to weigh LOC factors equally.³⁰⁸ However, this is not what happens in practice.³⁰⁹ When confronting complex decision processes, judges tend to limit the factors that they consider.³¹⁰ At some point, judges stop acquiring or analyzing new information. Instead, they simply commit to a decision and work backward to justify it. Some judges opt for a holistic weighing of the factors rather than attempting piecemeal arithmetic.³¹¹ Others emphasize case-by-case determination, and in so doing, underscore flexibility in applying a multitude of factors.³¹²

302. Beebe, *supra* note 21, at 1592 (“[T]he multifactor analysis has since become an essentially compulsory and formal exercise.”).

303. Restatement (First) of Torts §§ 729, 731 (1938).

304. *See, e.g.*, Helene Curtis Indus., Inc. v. Church & Dwight Co., Inc., 560 F.2d 1325, 1330 (7th Cir. 1977) (“In determining ‘likelihood of confusion’ several factors are important.”).

305. Beebe, *supra* note 21, at 1593; Richard A. Posner, *Judicial Behavior and Performance: An Economic Approach*, 32 FLA. ST. U. L. REV. 1259, 1271 (2005) (discussing judges’ aversion to being reversed).

306. Beebe, *supra* note 21, at 1582 (“Judges tend to ‘stampede’ these remaining factors to conform to the test outcome.”).

307. *See, e.g.*, Playtex Prods., Inc. v. Georgia-Pacific Corp., 390 F.3d 158, 162 (2d Cir. 2004) (finding no “single factor as dispositive”); Eli Lilly & Co. v. Natural Answers, Inc., 233 F.3d 456, 462 (7th Cir. 2000) (stating that the “factors are not a mechanical checklist”).

308. *See* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 322 (S.D.N.Y. 2003) (noting the tendency towards this type of application).

309. Anthony E. Chavez, *Using Legal Principles to Guide Geoengineering Deployment*, 24 N.Y.U. ENVTL. L.J. 59, 93 (2016) (“Decision makers, however, often do not apply multi-factor—or multi-principle—tests as they are intended.”).

310. Beebe, *supra* note 21, at 1601.

311. Noble v. United States, 231 F.3d 352, 359 (7th Cir. 2000) (“[R]ather, courts must engage in a totality of circumstances approach.”).

312. John S. Applegate, *Worst Things First: Risk, Information, and Regulatory Structure in Toxic Substances Control*, 9 YALE J. REG. 277, 302 (1992).

Studies show that neither judges nor experts manage the exercise of integrating multifactor test (MFT) factors well.³¹³ Coherence-based reasoning causes consistent and predictable mistakes regardless of the identity, background, or motives of the judges or other extrinsic values beyond the essential cognitive machinery that every human being brings to complex decisions.³¹⁴ It may occur early in the decision-making process, and a single attribute can trigger coherence-based reasoning.³¹⁵

As a result, courts weigh those factors impressionistically. Beebe's study confirms judges in LOC cases employ "'fast and frugal' heuristics to short-circuit the multifactor analysis."³¹⁶ According to Beebe, doing so "is evidence . . . of human ingenuity rather than human fallibility,"³¹⁷ because "as consummate pragmatists, they 'take the best,' a strategy which empirical work suggests is an altogether successful—and rational—approach to decision-making."³¹⁸

Coherence-based reasoning leads judges to determine outcomes based on a few factors and then read other factors into the question to support that finding of infringement. It operates bidirectionally to fit together how a judge decides the factors should go together,³¹⁹ both preceding the decision and that which forms the basis for it.³²⁰ In the context of this Article, judges assessing evidence in LOC tests will look at them non-independently relative to the final decision. The resulting decision is biased, because as Dan Simon explains, "the hard case morphs into an easy one."³²¹ The takeaway is that an overload of factors demands too much from judges and forces them to stampede over

313. See, e.g., Robyn M. Dawes, *The Robust Beauty of Improper Linear Models in Decision Making* 34 AM. PSYCH. 571, 575 (1979).

314. See Chris Guthrie, Jeffrey J. Rachlinski & Andrew J. Wistrich, *Inside the Judicial Mind*, 86 CORNELL L. REV. 777, 778–80 (2001).

315. See Simon, Krawczyk & Holyoak, *supra* note 320, at 331 (suggesting that a single variable can initiate spreading coherence).

316. *Id.* at 1635. Tierney, *supra* note 107, at 235–36 ("[M]uch of the time spent going through the list of factors in any given case is in reality just an attempt to justify a predetermined conclusion about the likelihood of confusion.").

317. Beebe, *supra* note 21, at 1603.

318. Beebe, *supra* note 21, at 1604 n.88.

319. Simon, *supra* note 43, at 514–16.

320. See, e.g., Dan Simon, Chadwick J. Snow & Stephen J. Read, *The Redux of Cognitive Consistency Theories: Evidence Judgments by Constraint Satisfaction*, 86 J. PERSONALITY & SOC. PSYCHOL. 814, 830 (2004) ("Not only does the evaluation of the evidence influence the eventual verdict, but the developing verdict also seems to affect the evaluation of the evidence.").

321. Simon, *supra* note 43, at 517 (describing studies where coherence-based reasoning caused subjects who found for the defendant and those who found for the plaintiff to be more confident the evidence supported their view after they had issued their verdict).

those they deem less significant. In the absence of direct evidence of confusion, courts must ascertain it through a host of proxy factors.³²² The implications are as startling as they are important. Despite the urging by appeals courts, judges do not approach LOC robotically and discretely, summing them up on a mental ledger instead of using interrelated analyses. Instead, as a strategy for navigating complexity, LOC tests become mere smokescreens for judges to create an appearance of coherence resting on a small number of probative factors. Judges aim to employ simplified decision-making to reach satisfactory rather than optimal decisions.³²³ By recognizing that judges cherry-pick, we can make decisions simpler and limit factors while also driving out the error of discretion. This minimizes burdens on judges unwilling or unable to conduct deep investigations into every factor prescribed by the LOC standard in that circuit. After analyzing the applicable factors, courts could resolve cases by weighing the factors pointing in each direction.³²⁴ The key to simplifying confusion then is to concentrate on a few factors and help judges use them well.

The circuit courts currently use an average of 7.5 LOC factors, but far fewer are necessary.³²⁵ For a start, eliminate the LOC factors that cluster and overlap. The Restatement of Unfair Competition groups LOC factors into “actual confusion,” “market factors,” and “intent.”³²⁶

Beebe recommended three or four “core factors” informing “consumer perception in the marketplace rather than judicial perception in the courtroom.”³²⁷ Alejandro Mejías went further, stating that:

“[P]rincipally concentrating the analysis on the main two factors, similarity of marks and proximity of goods, adding any other relevant factors, instead of using unmanageable and misleading large lists of factors that are extremely difficult to balance, seems to be more in line with the thesis of scientific research on decision-making.”³²⁸

322. Laura A. Heymann, *The Reasonable Person in Trademark Law*, 52 ST. LOUIS U. L.J. 781, 783 (2008).

323. Russell B. Korobkin & Thomas S. Ulen, *Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics*, 88 CALIF. L. REV. 1051, 1077–78 (2000).

324. See Beebe, *supra* note 21, at 1601 (explaining how courts ordinarily weigh each factor in a balancing test).

325. See Beebe, *supra* note 21, at 1603.

326. RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 20–23 (1995) (market factors consist of: (1) the degree of similarity between the marks, (2) the degree of similarity in the marketing methods and channels of distribution, (3) the degree of care of prospective purchasers, (4) the degree of the senior mark’s distinctiveness, (5) the likelihood of bridging the gap, and (6) the geographic differences between the marks.).

327. Beebe, *supra* note 21, at 1646.

328. Mejías, *supra* note 103, at 348 (concentrating the analysis on the main two factors).

Intent and mark strength are overly malleable and distract from the base inquiry on consumer confusion. Other factors may be redundant. For instance, the similarity of products and services are market and geographic proximity proxies³²⁹ and mark strength nests within actual confusion.³³⁰ It might be argued that since courts disregard most extraneous factors, there is little harm in retaining them. However, scholars warn that even “rarely-dispositive factors pose the risk that they may lead courts astray.”³³¹

Beebe also recommended assigning weights to these factors. “To emphasize that the multifactor inquiry is an empirical—rather than formal— inquiry that seeks to determine the likely perception of consumers in the marketplace.”³³² By looking at only a few factors, courts can give their attention to the most pivotal considerations. Giving courts more bandwidth enables them to focus on what kinds of trademark uses they favor. They could identify positive externalities or socially valuable uses they want to reward despite potential harm to consumers or trademark owners.

Copyright law’s fair use defense uses a similar approach. The Copyright Act enumerates four factors and includes an open-ended preamble listing specific types of uses deemed fair.³³³ To complete the analysis, courts first determine whether the use qualifies as fair and may add to the list of presumptively fair uses as long as the new uses are referential.³³⁴ Next, courts use four questions, including how the alleged infringer used the copyrighted content, to determine if the use was fair or not.³³⁵ Again, doing so balances copyright owners’ interests against those of society in deciding how expressive works should be used within the framework.³³⁶

329. *See* Gucci Am., Inc. v. Gucci, No. 07-CIV.-6820-RMB-JCF, 2009 WL 8531026 *6 (S.D.N.Y. Aug. 5, 2009).

330. Dayoung Chung, *Law, Brands, and Innovation: How Trademark Law Helps to Create Fashion Innovation*, 17 J. MARSHALL REV. INTELL. PROP. L. 492, 568 (2018) (“Naturally, if plaintiff has evidence of actual confusion, the strength of the actual confusion evidence will weigh in favor of the plaintiff to find a likelihood of confusion.”).

331. Liu, *supra* note 104, at 579.

332. Beebe, *supra* note 21, at 1647; *see also id.* at 1646 (“[T]he order in which the factors are listed should reflect as much as possible the weight that should be given to them.”).

333. The four factors that judges consider are: (1) the purpose and character of the use; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion taken; and (4) the effect of the use upon the potential market. 17 U.S.C. § 107.

334. *See* Lloyd L. Weinreb, *Fair Use*, 67 FORDHAM L. REV. 1291, 1298–99 (1998) (questioning whether stated uses are presumptively fair).

335. *Id.* (interpretation depends on reading factors as either an exclusive list or guiding tools with factor analysis).

336. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 448 n.31 (1984) (“[S]ection 107 offers some guidance . . . However, the endless variety of situations . . . precludes the formulation of exact rules . . . The bill endorses the . . . general scope of . . . fair

Should we then conclude that efficiency equates to relevance? The danger here, as Beebe warned, is that decision-makers may “sacrifice,” or “consider a finite amount of information, maybe as few as two or three factors, to reach a good enough approximation of ‘correct’ outcomes.”³³⁷ Moreover, the factors to focus on first will depend on a judge’s view of its salience.³³⁸ That focus will gravitate toward the most familiar or concrete factors, which will, in turn, have an outsized influence on the outcome.³³⁹ Simultaneously, courts marginalize less familiar factors or those more difficult to ascertain. The next Section explains the basis for this Article’s rules of thumb to simplify the LOC tests.

V. RULES OF THUMB

Mark similarity, the similarity of goods and services, and evidence of actual confusion anchor the LOC analysis as the most relevant factors.³⁴⁰ Safe harbors protect core policies most in danger of being invaded by trademark expansionism while making it simpler and cheaper for businesses to do their due diligence and comply with the law.³⁴¹ The Troika of LOC factors—actual confusion, similarity, and proximity of services or products—and the twin safe harbors can leverage existing AI deep learning techniques, assigning weights to each factor and considering this weighted range of possibilities.³⁴² AI can also help mitigate coherence-based reasoning by getting judges to consider the weaknesses in their positions and the merits of opposing views.³⁴³

A. TRADEMARK’S TROIKA

A small set of key factors helps structure the LOC inquiry and gives notice of pertinent issues and relevant evidence and a more solid basis for predicting case outcomes. Courts should adopt this new formulation of the trademark factors. As Grynberg noted, “[e]ven if judges do no more than apply heuristics of questionable quality to the disposition of trademark claims, channeling the process through a consistent framework aids litigants in identifying and

use, but there is no disposition to freeze the doctrine . . . [since] courts must be free to adapt the doctrine to particular situations.”).

337. Maggie Gardner, *Parochial Procedure*, 69 STAN. L. REV. 941, 959 (2017).

338. Adrian Vermeule, *Three Strategies of Interpretation*, 42 SAN DIEGO L. REV. 607, 628 (2005) (“[A] heuristic that causes decisionmakers to overweight the importance of vivid, concrete foreground information and to underweight the importance of abstract, aggregated background information.”).

339. See Schauer, *supra* note 105, at 894–96 (discussing the distorting effect of salience on common law rulemaking).

340. See *infra* Section IV.A.

341. See *infra* Section IV.B.

342. See *infra* Section IV.C.

343. See *infra* Section IV.C.

accommodating the factors that guide factfinding.”³⁴⁴ The question then is, how many factors should we retain? Courts should retain three of the seven Polaroid factors because historically these are the ones judges find most probative.³⁴⁵

The first factor is actual confusion. Actual confusion is the most direct and decisive evidence of confusion.³⁴⁶ As a policy lever, it gives courts the ability to anchor their analysis in real-world characteristics. In addition, the evidence is pre-existing, does not depend on the vagrancies of survey design, and should make it easier for courts to dispose of cases pretrial.³⁴⁷

The second factor is mark similarity. Beebe found it was “by far the most influential” factor.³⁴⁸ Eighty-three percent of plaintiffs in injunction cases who won the similarity factor won the test, with ninety percent in plaintiff summary judgment motions.³⁴⁹ In applying it, courts judge similarity between marks holistically and in isolation based on consumers encountering them in the marketplace.³⁵⁰

Coherence-based reasoning is at play with the similarity factor, but with a twist, and in a good way. Courts use sights, sounds, and meaning to make snap judgments about mark similarity.³⁵¹ These heuristics allow judges to rely on “a

344. Michael Grynberg, *The Judicial Role in Trademark Law*, 52 B.C. L. REV. 1283, 1305 (2011).

345. Beebe, *supra* note 21, at 1601 n.88 (“Like any human decision makers, district judges attempt to decide both efficiently and accurately. In pursuit of efficiency, they consider only a few factors. In pursuit of accuracy, they consider the most decisive factors.”).

346. Beebe, *supra* note 21, at 1608 (finding a ninety-two percent plaintiff success rate). *See also* John Benton Russell, *New Tenth Circuit Standards: Competitive Keyword Advertising and Initial Interest Confusion in 1-800 Contacts v. Lens.com*, 30 BERKELEY TECH. L.J. 993, 1000 (2015) (“[C]ourts across several circuits view this as the strongest evidence a plaintiff can present in a trademark infringement case.”); Mark D. Robins, *Actual Confusion in Trademark Infringement Litigation: Restraining Subjectivity Through a Factor-Based Approach to Valuing Evidence*, 2 NW. J. TECH. & INTELL. PROP. 117, 1 (2004) (“In a case where all other circumstances point to a finding of non-infringement, significant evidence of actual confusion dramatically alters the equation.”).

347. I am grateful to Jon Lee for this insight.

348. Beebe, *supra* note 21, at 1600.

349. Beebe, *supra* note 21, at 1625.

350. The similarity between the marks makes it more likely consumers will become confused as to the source. Extremely similar marks or goods may suggest counterfeiting and free riding. Parodies, comparative advertising, and nominative use make consumers less likely to be confused, even if the third party uses the identical term. Defendants can easily compare visual or aural elements in context, making this a useful factor to encourage due diligence. *See* MCCARTHY, *supra* note 13, § 23:21 (discussing the “sound, sight, and meaning” test for mark similarity).

351. Adam M. Samaha, *Looking over A Crowd—Do More Interpretive Sources Mean More Discretion?*, 92 N.Y.U. L. Rev. 554, 614 (2017) (“[A]ccurately estimating the probability of

small set of cheap and reliable factors that are close enough to the ideal.”³⁵² Adam Samaha approves of this approach, since “[p]rioritizing the judge’s impressions about the similarity of marks, therefore, tends toward the high values of trademark law at bargain-basement prices.”³⁵³

The third factor is the proximity of services or products. It tells courts how likely consumers are to assume an association between the marks used on related products.³⁵⁴ Confusion is more likely when an accused product contains multiple indicia of similarity. For instance, house brands typically include house marks, product-specific brands, product packaging, and color or configuration.³⁵⁵ Conversely, consumers are less likely to be confused when defendants copy only a few elements.³⁵⁶ Beebe noted that the lack of proximity of the parties’ goods was “decisive” to the outcome.³⁵⁷

Courts look to the trademarked product, the relevant market, as well as potential consumers.³⁵⁸ Product proximity overlaps substantially with marketing and advertising channels and should be subsumed within those channels. For this reason, proximity can serve as an omnibus factor for other factors such as the relative quality of goods sold, bridging the gap between the relevant public’s perspective (rather than from the legitimate aspirations of the trademark owner), and similarity of distribution channels.

consumer confusion can require a snap judgment, which often is how consumers actually formulate impressions and make purchasing decisions.”).

352. *Id.* at 614.

353. *Id.*

354. *Virgin Enters. Ltd. v. Nawab*, 335 F.3d 141, 150 (2d Cir. 2003).

355. *See, Lemley & McKenna, supra* note 86, at 433 (“For example, producers often distinguish their goods with a house mark, a product-specific brand, a logo, a slogan, product packaging, and perhaps product color or configuration all at once.”).

356. George Miaoulis & Nancy D’Amato, *Consumer Confusion and Trademark Infringement*, 42 J. MKTG. 48, 54 (1978) (finding, in the context of competing goods, that the primary cue for association between two brands was not the name but the visual appearance).

357. Beebe, *supra* note 21, at 1600.

358. *Best Cellars, Inc. v. Grape Finds at Dupont, Inc.*, 90 F. Supp. 2d 431 at 456 (S.D.N.Y. 2000).

Table 2: Revised LOC Factors

<i>Polaroid</i> Factors	Troika Factors
Strength of the plaintiff's mark	Discard
Similarity of plaintiff's and defendant's marks	Retain
Competitive proximity of products or services	Retain
Likelihood plaintiffs will "bridge the gap" and offer a product like a defendant's	Discard
Actual confusion	Retain
Defendant's good faith	Discard
Quality of defendant's product	Discard because covered by competitive proximity of products or services.
Buyer sophistication	Discard because covered by actual confusion.

The Troika moves trademark doctrine a step in the right direction by limiting ad-hoc fact-finding. However, this is not enough. We also need to identify safe harbors. It is difficult even for savvy parties to predict the outcome in advance and resolve disputes early in any court proceeding, placing swathes of activity at significant risk.³⁵⁹

B. SAFE HARBORS

Safe harbors protect the uses of the marks for commentary, parody, or comparison. The First Circuit noted that trademarks "form an important part of the public dialog on economic and social issues."³⁶⁰ As trademarks expand beyond source identification, they seed public discourse with their

359. Welkowitz, *supra* note 122, at 148 ("[T]he level and even the existence of confusion is difficult to predict in advance, partly due to the uncertainties built into trademark law's test for confusion, those who would engage in valued activity must do so at significant risk.").

360. Mark A. Lemley & Mark McKenna, *Irrelevant Confusion*, 62 STAN. L. REV. 413, 442 (2010); 6 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 31:146 (4th ed. 1994); *L.L. Bean, Inc. v. Drake Publishers, Inc.*, 811 F.2d 26, 30 (1st Cir. 1987) ("[T]rademarks offer a particularly powerful means of conjuring up the image of their owners, and thus become an important, perhaps at times indispensable, part of the public vocabulary.").

communicative value.³⁶¹ Trademark owners obtain rights with inchoate boundaries. When the public interacts with a trademark, the mark may become imbued with collective meaning. This collective meaning has social value. If a trademark has taken on this collective meaning, then in appropriate instances, the law should offer the owner of such a trademark categorical protection from lawsuits.³⁶²

Communication relies on a plethora of legally protected words, graphics, sounds, and smells.³⁶³ Beyond computers or smartphones, APPLE may represent a nonconformist hip lifestyle compared with users of LENOVO's more staid business offerings. Trademarks become tools of communication and expression, and the public helps shape their boundaries as they become symbols that embody culture itself.³⁶⁴ When trademark law becomes entangled with free speech, what qualifies as speech and protected speech becomes folded into the LOC standard inquiry.

LOC is relevant to determining whether the use is objectively fair and whether defendants use the term "otherwise than as a mark."³⁶⁵ Likewise, nominative fair use (referring to the trademark holder or its products) folds confusion into determining whether an expressive use "explicitly misleads" consumers or whether the use falsely suggests source or sponsorship.³⁶⁶

The law adopts a balancing test, known as the *Rogers* test for expressive uses.³⁶⁷ The *Rogers* test balances "the public interest in avoiding consumer confusion" against "the public interest in free expression."³⁶⁸ Cases applying

361. See Kozinski, *supra* note 73, at 973–74 (Noting how businesses inject the "effervescent qualities" of trademarks "into the stream of communication with the pressure of a firehose by means of mass media campaigns.").

362. See, e.g., William McGeeveran & Mark P. McKenna, *Confusion Isn't Everything*, 89 NOTRE DAME L. REV. 253, 301–06 (2013) (proposing categorical exclusions for some favored uses).

363. Diamond & Franklyn, *supra* note 255, at 2031.

364. See Beebe, *supra* note 80, at 624 (arguing trademark law is both an economic doctrine and "a semiotic doctrine elaborating the principles of sign systems, of language").

365. See, e.g., *KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc.*, 543 U.S. 111, 118–23 (2004).

366. *Rogers v. Grimaldi*, 875 F.2d 994, 999 (2d Cir. 1989).

367. 15 U.S.C. § 1115(b)(4) (allowing the public "fair uses" "in good faith only to describe the goods or services."); see William McGeeveran, *Rethinking Trademark Fair Use*, 94 IOWA L. REV. 49, 100 (2008) (discussing *Rogers* test); see, e.g., *Mattel, Inc. v. Walking Mountain Prods.*, 353 F.3d 792, 816 (9th Cir. 2003) (noting that the defendant's nominative fair use implicates "free expression").

368. *Rogers*, 875 F.2d at 999.

the test credit minimal artistic relevance and focus on the defendant's conduct to determine whether a use misleads consumers.³⁶⁹

McGeveran observed that expressive uses of trademarks were “a scenario that the originators of the test never contemplated.”³⁷⁰ The risk of chilling such socially beneficial uses has not been limited to small businesses or individuals. Movie studios use them to portray the real world realistically. Even large institutions like Hollywood studios adopt policies to manage the risk of litigation over unauthorized trademark use. Implant rights clearance and licensing adds significant costs to the production of artistic expression.³⁷¹

While the costs of impinging free speech are high, the costs of being overly permissive in expressive use cases cause only minimal harm or are rare, or both.³⁷² Research on brand extensions shows owners are rarely harmed by consumers' mistaken association of unrelated products. Consumers rarely alter how they see the brand quality when they encounter negative information about products offered under the same mark.³⁷³ The negative impact stays with the related products but does not corrupt a positive view of the owner's line of products.³⁷⁴ Safe harbors protect the uses of the marks for commentary, parody, or comparison.³⁷⁵

Expressive uses for commentary, parody, or education should fall within safe harbors.³⁷⁶ Critiquing products or corporate behavior requires us to use

369. See, e.g., *Brown v. Elec. Arts, Inc.*, 724 F.3d 1235, 1243–46 (9th Cir. 2013) (finding a likeness of Jim Brown artistically relevant to Electronic Arts's video game and holding that the degree of relevance need “merely . . . be above zero”); *Louis Vuitton Malletier S.A. v. Warner Bros. Ent. Inc.*, 868 F. Supp. 2d 172, 178 (S.D.N.Y. 2012) (“The threshold for ‘artistic relevance’ is purposely low and will be satisfied unless the use has no artistic relevance to the underlying work whatsoever.”).

370. William McGeveran, *The Trademark Fair Use Reform Act*, 90 B.U.L. REV. 2267, 2269 (2010).

371. *Id.* at 2276 (“But many institutions have determined that the potential cost of defending a lawsuit is too high, even when discounted for the low likelihood of getting sued and the very low likelihood of paying damages.”).

372. *Id.* at 2286.

373. *Id.*

374. *Id.* at 430 (“Consumers, in other words, are smart enough to distinguish different products and hold different impressions of them.”).

375. See, e.g., *KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc.*, 543 U.S. 111, 123 (2004) (finding that confusion is relevant to whether descriptive use is “fair”); *New Kids on the Block v. News Am. Publ'g, Inc.*, 971 F.2d 302, 308 (9th Cir. 1992) (noting that confusion is relevant to nominative fair use).

376. See Andy Greene, *Nathan Fielder Talks ‘Dumb ‘Starbucks’ and Pranking Instagram*, ROLLING STONE (July 24, 2014), <http://www.rollingstone.com/movies/news/nathan-fielder-talks-dumb-starbucks-and-pranking-instagram-20140724>.

them.³⁷⁷ This Article proposes establishing two safe harbors for potential likelihood of confusion issues. The first safe harbor should be expressive uses of protected trademarks. Expressive uses for commentary, parody, or education should fall within safe harbors. Critiquing products or corporate behavior also requires us to use trademarks. The second should be referential uses of trademarks. Nominative fair use by the trademark holder or its products should not trigger liability. Rivals and repair services need to make referential uses to compete and advertise their services to the public. The law recognizing comparative uses as a defense to referential use should still apply but it should go no further.” Rivals and repair services need to make referential uses to compete and advertise their services to the public.³⁷⁸ The law currently recognizes comparative uses as a defense but should go further.³⁷⁹

Using a single static meaning as defined by the trademark owner sacrifices the ability of consumers to evaluate rival goods and services.³⁸⁰ The risk is that plaintiffs can shut down consumer groups challenging its corporate practices and stave off rivals advertising alternative products that consumers may prefer.³⁸¹ Even when a term has a descriptive meaning, it can be difficult to determine because meanings depend on perspective and context.³⁸² Individuals may use a term that is part of a trademark to describe something completely different and separate. For rulemaking, there is no basis for a presumption of harm involving noncompeting goods even if there is confusion. Trademarks are vital for the public to share product reviews, views on a company’s labor practices, and other qualities of a business. Requiring the user to refer to the mark owner obliquely would be inefficient.

Safe harbors offer advantages over attempts to prescribe clear rules. These include improving predictability and ease of determination, allowing courts to resolve issues sooner in the litigation process. Here, Gideon Parchomovsky

377. See *New Kids on the Block*, 971 F.2d at 307 (“Much useful social and commercial discourse would be all but impossible if speakers were under threat of an infringement lawsuit every time they made reference to a person, company or product by using its trademark.”).

378. See, e.g., *Toyota Motor Sales, U.S.A., Inc. v. Tabari*, 610 F.3d 1171, 1180–82 (9th Cir. 2010) (allowing automobile broker specializing in facilitating Lexus purchases to use LEXUS mark as part of domain name).

379. See, e.g., *Smith v. Chanel, Inc.*, 402 F.2d 562, 563 (9th Cir. 1968) (holding that truthful comparative advertising is not trademark infringement).

380. See Graeme W. Austin, *Trademarks and the Burdened Imagination*, 69 BROOK. L. REV. 827, 828–29 (2004).

381. See generally Mark A. Lemley & Mark P. McKenna, *Is Pepsi Really a Substitute for Coke? Market Definition in Antitrust and IP*, 100 GEO. L.J. 2055, 2111–12 (2012).

382. See, e.g., Richard Craswell, *Interpreting Deceptive Advertising*, 65 B.U. L. REV. 657, 668–78 (1985) (emphasizing the importance of pragmatic inferences in interpreting the meaning of advertisements).

and Alex Stein make a more general point that “[r]eplacing these criteria with rules that will lay down irrebuttable presumptions of consumer confusion, or lack thereof, could make litigation over trademarks cheaper than it presently is.”³⁸³ The case is over as soon as the defendants demonstrate a basic fact.³⁸⁴

Safe harbors already exist within trademark law, even if not specifically within the LOC tests. For instance, the law does not protect functional product designs to avoid giving plaintiffs an advantage against rivals unrelated to the plaintiff’s reputation.³⁸⁵ Similarly, the law keeps plaintiffs on a leash so they cannot monopolize trademarks with descriptive words and receive protection for generic terms.³⁸⁶

Safe harbors for expressive and descriptive uses allow courts to dispose of LOC cases more simply and justly. For example, uses that fit the conventional way descriptive terms are used in ordinary language would give prospective users an advantage in establishing descriptive use and exiting litigation early, thereby avoiding high litigation costs. In addition, they help carve out pockets of strong protection and guide the development of trademark rights in other areas such as merchandising rights, without giving owners the right to rely upon LOC to justify its approval. At its heart, the LOC represents a probability that a defendant’s use of its trademarks will confuse consumers.³⁸⁷ Trademark’s Troika of actual confusion, mark similarity, and similarity of goods and services paves the road for AI to fill the final piece of the equation to simplify LOC.

C. POWERED BY ARTIFICIAL INTELLIGENCE: HOW TO CATALYZE TRADEMARK REFORM PROPERLY

This Section sketches a roadmap to implementing AI to catalyze trademark reform. AI describes an algorithm capable of mimicking mental functions that we associate with the human mind, including learning and problem-solving.³⁸⁸ First, this Section discusses why and how AI is helpful to trademark disputes. Second, this Section makes three suggestions for how to use AI to ensure this Article’s proposal for trademark reform is effective: predictive analysis, robot

383. Gideon Parchomovsky & Alex Stein, *Catalogs*, 115 COLUM. L. REV. 165, 178 (2015).

384. See Welkowitz, *supra* note 122, at 168 (referencing Fed. R. Evid. 301).

385. 15 U.S.C. § 1052(e)(5).

386. See *Abercrombie & Fitch Co. v. Hunting World, Inc.*, 537 F.2d 4, 9 (2d Cir. 1976) (“[e]ven proof of secondary meaning, by virtue of which some ‘merely descriptive’ marks may be registered, cannot transform a generic term into a subject for trademark.”).

387. Leah Chan Grinvald, *Shaming Trademark Bullies*, 2011 WIS. L. REV. 625, 636 (2011) (“This liability standard refers to the probability (not the actuality or possibility) that consumers will be confused by the same or similar trademarks.”).

388. *Quick Check*, WESTLAW, <https://legal.thomsonreuters.com/en/products/westlaw-edge/quick-check> (last visited Jan. 6, 2023).

judges, and a weighing of factors. Third, this Section suggests a method for weighing the LOC factors systematically.

As seen with LOC, where the criteria are vague and multiple values are at play, different judges can apply LOC differently, making it a quintessential example of a “noisy” standard. Moreover, basing outcomes on a likelihood means they may not reflect true assessments of whether consumers would indeed have been confused. To reduce bias and noise, Kahneman, Sibony, and Sunstein recommend considering using algorithms in decision-making.³⁸⁹ They point out that algorithms are “noise-free,” explaining that they produce the same results every time if the dataset remains the same.³⁹⁰ Furthermore, research in multiple studies, including radiology, recruitment and financial advisory work, validates that AI-assisted analyses lead to better outcomes than human judgment alone.³⁹¹

In 2021, Westlaw unveiled its Quick Check document analysis tool. Quick Check allows users to securely upload a brief and then analyzes the brief with its proprietary AI powered by a deep learning algorithm. The algorithm analyzes text and citations to explore all avenues of research, including relevant authority overlooked by traditional research.³⁹² In addition, AI identifies patterns and connections users may not detect themselves.³⁹³ These include citations that would otherwise receive negative KeyCite treatment, along with relevant language from that case, so users can determine whether the treatment affected a case for a relevant reason.³⁹⁴ In short, Quick Check enables judges or attorneys to determine the merits of a case efficiently.

389. See KAHNEMAN ET AL., *supra* note 3, at 135.

390. See KAHNEMAN ET AL., *supra* note 3, at 135.

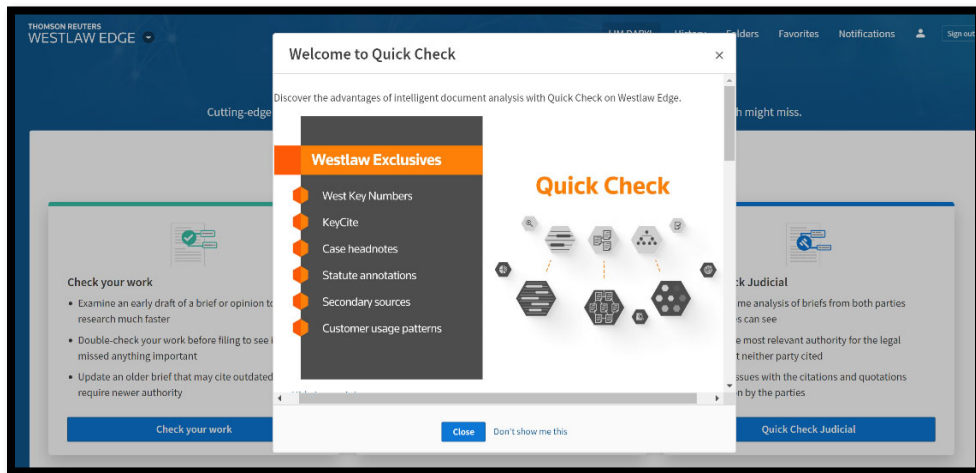
391. KAHNEMAN ET AL., *supra* note 3, at 28-29, 132, 280.

392. WESTLAW, *supra* note 388.

393. WESTLAW, *supra* note 388.

394. WESTLAW, *supra* note 388.

Figure 1: Westlaw's AI-Powered Quick Check Application



Quick Check represents stunning progress from ancient times when research meant pouring over volumes of printed case reporters in libraries. It powerfully illustrates the ability of machines to learn salience and apply it to new data. With machine learning, the algorithms improve as they are exposed to more data. Breathtakingly, Quick Check also keeps sight of underlying tradeoffs, particularly those that are only evident through a comprehensive survey of case law.³⁹⁵ These include constitutional concerns, anti-competitive concerns, and trademark law encroaching on other areas of intellectual property.³⁹⁶

AI has also penetrated trademark practice. In 2019, Singapore launched Intellectual Property Office of Singapore IPOS Go (“IPOS Go”), the world’s first mobile app for trademark filing.³⁹⁷ IPOS Go integrates AI technology to search for similar trademarks on the trademark register, allowing applicants to preempt possible objections from similar existing trademarks.³⁹⁸ Judges or judicial law clerks feeding party briefs through a system combining features

395. WESTLAW, *supra* note 388.

396. *See* *Specialized Seating, Inc. v. Greenwich Indus., L.P.*, 616 F.3d 722, 727 (7th Cir. 2010) (“Another goal [of functionality], as *TrafFix* stressed, is to separate the spheres of patent and trademark law, and to ensure that the term of a patent is not extended beyond the period authorized by the legislature.”).

397. *IPOS Go Mobile*, INTELL. PROP. OFF. SING., <https://www.ipos.gov.sg/eservices/ipos-go> (last visited Jan. 6, 2023).

398. Tim Lince, *Innovation at the Singapore IP Office: Spotlight on Non-core Tools and Services*, WORLD TRADEMARK REV. (Aug. 5, 2020), <https://www.worldtrademarkreview.com/governmentpolicy/innovation-the-singapore-ip-office-spotlight-non-core-tools-and-services>.

from Quick Check and IPOS Go can quickly identify which side the prevailing law favors and why.

Judges applying a LOC standard may define the scope of trademark rights under the guise of factfinding. For instance, intent plays an outsized role in outcomes even though it has a tangential relationship to the core question of whether consumers are likely to be confused.³⁹⁹ Algorithmically determining confusion allows the legal system to simplify trademark adjudication and lower the incidence of judicial errors. Making LOC more rule-like, both through the doctrinal reformation of the standard and through the application of AI, makes it easier for appeals courts to scrutinize and overturn deviant lower court decisions and allows lower courts to distinguish dubious precedent based on facts.⁴⁰⁰

The algorithm is a tool for judges and does not replace them.⁴⁰¹ AI systems like Quick Check and IPOS Go augment stakeholders' decision-making and still need to pick between recommended outcomes manually. Then, the courts can examine the record below, including the AI system's recommendations on appeal. However, the system needs three more additions to catalyze trademark reform properly: predictive analytics, the robot judge, and how to weigh the factors.

1. *Predictive Analytics*

First, if the law was merely a set of rules, processing it through algorithms makes sense, just as we would use a calculator rather than do long division by hand. However, the law regulates human behavior embedded with contested values existing in a dynamic landscape. As Oliver Wendell Holmes said, "The life of the law has not been logic: it has been experience."⁴⁰² The algorithm would need to account for case law changes over time.⁴⁰³

AI systems like Quick Check process legal rules in fixed systems top-down. A more sophisticated version of the system needs to run on deep learning algorithms available today to analyze vast amounts of data from the bottom

399. See *supra* Part IV.B.

400. See Frederick Schauer, *Formalism*, 97 YALE L.J. 509, 541–42 (1988) (noting errors are more easily detectable under rules).

401. *Id.* at 574. (The expert chooses the variables and determines what to look for. The linear model integrates the information.)

402. OLIVER WENDELL HOLMES, JR., *THE COMMON LAW* 3 (M. Howe ed., 1963).

403. Chan Grinvald, *supra* note 387, at 633 (2011) ("The trademark of the twenty-first century bears little resemblance to the trademark of the late nineteenth century."); *Compare* Qualitex Co. v. Jacobson Prods. Co., 514 U.S. 159, 162 (1995) (almost anything can function as a trademark if source identifying) *with* A. Leschen & Sons Rope Co. v. Broderick & Bascom Rope Co., 201 U.S. 166, 171 (1906) ("[A] trade-mark which may be infringed by a streak of any color, however applied, is manifestly too broad.").

up. The goal is to offer AI predictions based on experience beyond the correct answer in an individual case.

Our ability to reason in the abstract gives us systematic superiority over AI performance thus far.⁴⁰⁴ Machine learning models typically cannot find commonalities between the possible options when variables are uncertain.⁴⁰⁵ However, things are changing. Recently, the progress in deep learning algorithms allows machines to predict human behavior and better coordinate actions with ours. In 2021, after analyzing thousands of hours of movies, sports games, and shows, Carl Vondrick revealed an astonishingly accurate algorithmic prediction method,⁴⁰⁶ the Vondrick algorithm, that predicts hundreds of activities, from handshaking to fist-bumping.⁴⁰⁷

Vondrick's algorithm enables machines to organize variables independently,⁴⁰⁸ adjusting for specificity based on the level of certainty in the variables it observes.⁴⁰⁹ Applied to the trademark context, this algorithm could classify marks according to their international classifications, streams of commerce, and visual, aural, or other sensory dimensions. These AI capabilities can help better mimic consumer perception and behavior, giving judges a more accurate baseline for finding or exonerating liability.

What would the technical rollout look like? Structurally, law firms could use API that interfaces with the court system, like e-filing protocols already in place today. Lexis, Westlaw, or Bloomberg could help develop that system, and integrate it into their database of cases, briefs, and articles. Individual lawyers can use other devices, such as their smartphones, computers, and cars, which function as object-detection networks.⁴¹⁰ The network takes an image as input and returns a list of values representing the image's probability of belonging to several classes. For example, if data scientists want to train a neural network to detect all forty-five trademark classes in the USPTO's classification system, the output layer will have forty-five numerical outputs, each containing the probability of the image belonging to one of those classes.⁴¹¹

404. Holly Evarts, Columbia Engineering, *AI Learns to Predict Human Behavior from Videos* (June 28, 2021), <https://www.engineering.columbia.edu/press-release/ai-learns-to-predict-human-behavior-from-videos>.

405. *Id.*

406. *Id.*

407. *Id.*

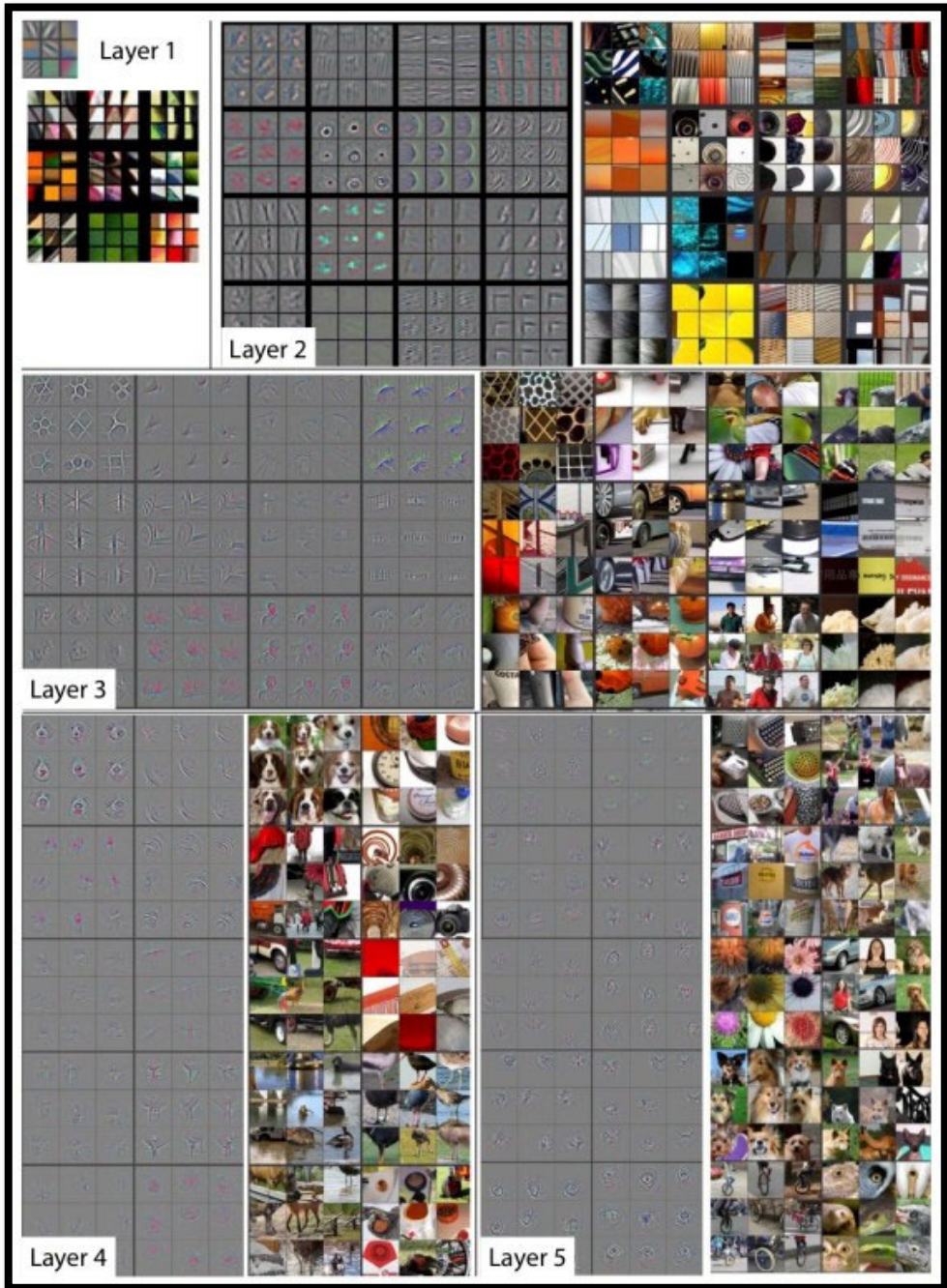
408. *Id.*

409. *Id.*

410. Ben Dickson, *An Introduction to Object Detection with Deep Learning*, TECH TALKS, (June 21, 2021), <https://bdtechtalks.com/2021/06/21/object-detection-deep-learning/>.

411. *Id.*

Figure 2: Image Recognition



If images are at issue, for instance, the AI asks a series of questions, parties can input an image, and the AI can search against case law and tell the parties whether the image infringes.

Realistically, not all trademark disputes are amenable to AI resolution. Some cases may be more complex, making it hard to resolve claims at an early stage of litigation. For example, the facts may require the fact finder to consider if the plaintiff's mark would fence off functional features rivals need to use. These might include color coding, industry design, and storage conventions. However, the perfect is the enemy of the good. Progress, not perfection, is what we seek.

2. *The Robot Judge*

Second, parties need to accept algorithmic adjudication for trademark law to reform properly. Kahneman, Sibony, and Sunstein's research show that professionals trust their intuition and doubt machines can do better, despite evidence to the contrary.⁴¹² People are more willing to accept human mistakes than mistakes by algorithms, even if algorithm mistakes are fewer.

Václav Havel argued:

[W]e have to abandon the arrogant belief that the world is merely a puzzle to be solved, a machine with instructions for use waiting to be discovered, a body of information to be fed into a computer in the hope that, sooner or later, it will spit out a universal solution.⁴¹³

Those like Havel may reject solutions like those that AI provides, believing cases are highly varied and that good judges address those variations—which might mean tolerating bias and noise or rejecting some strategies that reduce them by taking away their discretion. They must be persuaded because they are wrong.

Using AI within the justice system raises ethical concerns, including credibility, transparency, and accountability. There are also equity considerations since deep-pocketed clients with ever-closer ties to technology companies may better leverage automation. Society needs to trust it enough to adopt its recommendation to govern the rights of the parties.

This Article's response to the objection that AI is opaque and insufficiently accountable is to ask: "Relative to what better alternative means of adjudication?" Algorithms operate in a black box, but so do judges, and the

412. See KAHNEMAN ET AL., *supra* note 3, 144-46.

413. VACLAV HAVEL, *THE ART OF THE IMPOSSIBLE: POLITICS AS MORALITY IN PRACTICE—SPEECHES AND WRITINGS*, 91, 1990-96, (Paul Wilson et al., Trans., Alfred A. Knopf 1997).

trend of judges engaging in post hoc reasoning is well documented and discussed in Part III. AI provides a more objective anchor to tether the LOC analysis in the face of coherence-based reasoning.

Justice Breyer surmised that judges review their decisions with confidence, forgetting doubts or the possibility they might have gone the other way.⁴¹⁴ Dan Kahan explains that judicial opinions can be “notoriously—even comically—unequivocal” and rarely “acknowledge that an issue is difficult, much less that there are strong arguments on both sides.”⁴¹⁵ Because confirmation bias filters out new information that contradicts existing hypotheses,⁴¹⁶ equivocal information is likely to further drive those with divergent views apart as both sides misinterpret the evidence to confirm their opposing positions.⁴¹⁷ It is important for the losing party to feel heard. In building on the earlier case for a robot judge, AI can provide the basis for an online dispute resolution system with the judge as a second-level reviewer.

More specifically, the current trademark regime is not the paradigm of accountability either. As Grynberg observed,

[a] framework devised to channel ad hoc factual determinations into an intelligible framework becomes instead a vehicle for ad hoc lawmaking. The outcomes may or may not be substantively palatable, but they undermine accuracy (insofar as the legal inquiry takes the guise of a factual one) and the system goals of transparency and accountability.⁴¹⁸

Likewise, courts allow nominative fair use determinations to be derailed by consumer confusion.⁴¹⁹ Back in the trademark context, for instance, if a defendant uses the plaintiff’s mark to refer to the plaintiff, it is meaningless to compare mark similarity. Comparing trademarks based on “similarity” lowers the bar for plaintiffs to make their infringement case without fully discharging their burden. Additionally, courts are left with no guidance on when to shift the burden to the defendant to establish a defense.

414. *Justice Breyer: The Court, the Cases and Conflicts*, NAT’L PUB. RADIO (Sept. 14, 2010), <http://www.npr.org/templates/story/story.php?storyId=129831688>.

415. Dan M. Kahan, *Foreword: Neutral Principles, Motivated Cognition, and Some Problems for Constitutional Law*, 125 HARV. L. REV. 1, 59 (2011) (noting that this phenomenon is especially odd at the Supreme Court, where “the main criterion for granting certiorari is a division of authority among lower courts”).

416. Matthew Rabin, *Psychology and Economics*, 36 J. ECON. LITERATURE 11, 36 (1998).

417. Kahan, *supra* note 419, at 59–61.

418. Grynberg, *supra* note 119, at 1320.

419. *See Cairns v. Franklin Mint Co.*, 292 F.3d 1139, 1150–52 (9th Cir. 2002).

Kahneman, Sibony, and Sunstein also recommend designating a “decision observer” for complex decisions.⁴²⁰ The observer uses a checklist to spot biases in real-time.⁴²¹ As applied to LOC, the AI can function as a check on whether the judge neglected anything important, gave weight to something irrelevant, expressed bias towards a conclusion, considered alternatives, or relied upon anecdotes unsupported by the factual record. The authors also recommend that judges resist leaning on intuition before assimilating and analyzing a critical amount of information—intuition has its place, but as the authors put it, that intuition must be “informed, disciplined and delayed.”⁴²²

The literature is replete with evidence that linear modeling algorithms trump intuitive clinical judgment.⁴²³ In the same way, using the trademark Troika and safe harbors as its filters, the algorithm can recognize unenumerated instances with similar characteristics.⁴²⁴ Leadership should come from the bench and bar. They benefit from the aura of expertise described in the Introduction and have a responsibility to the rest of society to use the best tools available to do their jobs.

3. *Weighing the Troika Factors*

Third, there needs to be a method to weigh the Troika factors systematically for trademark reform to be effective, whether or not the Troika factors are adopted. The LOC factors had no weights assigned, eroding the ability to apply the tests objectively or in a manner that can be replicated.⁴²⁵ AI can help integrate data and provide a statistical prediction based on input variables. Humans are superior at selecting and coding information but poor at integrating it.⁴²⁶

When forecasting, Kahneman, Sibony, and Sunstein recommend assigning probabilities rather than absolute values or binary “yes” or “no” judgments.⁴²⁷ With LOC, numerical thresholds would serve this purpose and relying more

420. See KAHNEMAN ET AL., *supra* note 3, at 222, 240-43.

421. See KAHNEMAN ET AL., *supra* note 3, at 222, 240-43.

422. See KAHNEMAN ET AL., *supra* note 3, at 373.

423. This is seen, for example, in the case of banks predicting bankruptcies. Dawes, *supra* note 313, at 579.

424. See generally, Parchomovsky & Stein, *supra* note 383, at 182.

425. See *Menard, Inc. v. Commissioner*, 560 F.3d 620, 622–23 (7th Cir. 2009). (“Multifactor tests with no weight assigned to any factor are bad enough from the standpoint of providing an objective basis for a judicial decision; multifactor tests when none of the factors is concrete are worse.”).

426. Dawes, *supra* note 313, at 573.

427. See KAHNEMAN ET AL., *supra* note 3, 263 (“To many people, forecasting means the latter—taking a stand one way or the other. However, given our objective ignorance of future events, it is much better to formulate probabilistic forecasts.”).

heavily on rules, such as judicial sentencing guidelines, to reduce noise.⁴²⁸ The Troika factors, coupled with twin safe harbors, provide a similar framework for LOC analysis. On appeal, the variability of decisions reveals some idea of the extent of noise to the appellate court. A three-judge circuit appeals court or nine-Justice Supreme Court bench provides an additional check for this noise.

Computer scientists could build a model that requires judges to rate the three factors on a scale of 0-10. For instance, if the marks were completely different, the judge would rate it '0' (the lowest rating possible), but if the mark were simple counterfeits, the judge would rate it '10' (the highest rating). Thus, the algorithm would set a numerical threshold for finding confusion that maps to case law and the balance of probabilities. Over time, the algorithm will provide more granular information about the characteristics driving outcomes in LOC cases. In this way, the algorithm would imitate judges, granting a low score to a particular factor and consequently a lower success rate to plaintiffs.

AI can expand the scope of cases so that courts can dispense cases summarily. It can also avoid the risk of judges engaging in side-by-side mark comparison to ensure they apply the real-world purchasing context. Once these fundamentals are in place, future versions of the algorithm would perfect what surveys struggle to—capturing the collective perception of the relevant consumer group.

Importantly, the results from AI recommendations challenge judges' prior assumptions, providing a check against coherence-based reasoning. For example, Simon's research shows that confronting people with merits of the opposite side reduced the effect of coherence shifts by about fifty percent.⁴²⁹ In particular, his study moderated jury instruction by expressly requesting jury members to "take some time to seriously consider the possibility that the opposite side has a better case."⁴³⁰ Legal studies similarly showed that asking lawyers to consider the weaknesses in their side or reasons that the judge might rule against them mitigated bias.⁴³¹

To summarize, the algorithm would need to account for case law changes over time. Parties also need to accept algorithmic adjudication for trademark law to reform properly. Finally, there needs to be a way to weigh factors

428. See KAHNEMAN ET AL., *supra* note 3, 17-21.

429. Simon, *supra* note 43, at 543-44 (noting that "[m]ore studies are required to gain a better sense of the effects of the debiasing intervention.>").

430. Simon, *supra* note 43, at 570-71.

431. See Linda Babcock, George Loewenstein & Samuel Issacharoff, *Creating Convergence: Debiasing Biased Litigants*, 22 L. & SOC. INQUIRY 913, 920-21 (1997).

systematically for trademark reform to be effective, whether or not the Troika factors are adopted.

D. COURTS, NOT CONGRESS

It is worth pausing to address one potential objection to the idea that courts should be the ones implementing these rules of thumb. After all, Congress has a plenary perspective. Legislators may do better than courts in considering multifaceted interests. Moreover, courts are constrained by the case record and facts before them, limiting their ability to balancing broader interests.⁴³² For example, brand owners purport to show consumer confusion, but consumers' interests may be more nuanced and may even benefit from the court allowing the defendant's conduct.⁴³³ Thus, Grynberg noted:

[t]he primacy of the particular may unduly influence judicial decisions if the urgency of the facts at hand obscures the broader consequences of a requested holding. Resolving the case before the court creates binding precedent even when it is not fairly representative of future analogous situations.⁴³⁴

The biggest problem is that Congress would need to promulgate the LOC framework *ex ante* and make it specific enough to help courts identify conduct justifying intervention.⁴³⁵ LOC cases are too fact-specific for legislative rules to be of much use.⁴³⁶ And then there is inevitable ambiguity stemming more from the limitations of language than the draftsman's skill which may bring things back full circle.⁴³⁷ Even if well-drafted, the legislative process's numerous veto points create obstacles to correct the legislative error.⁴³⁸ Finally,

432. *New York v. Ferber*, 458 U.S. 747, 768 (1982).

433. Grynberg, *supra* note 119, at 1302 (“While plaintiffs are seen as vindicating the interests of confused consumers, defendants are rarely seen as performing a similar function for the non-confused, even though these consumer often have an interest in the continuation of the defendant’s conduct.”).

434. Grynberg, *supra* note 119, at 1301.

435. *See* Schauer, *supra* note 105, at 892 (“When there is no actual dispute, so the argument goes, everything is speculation, and speculation that is not rooted in real world events is especially likely to be misguided.”).

436. Michael Grynberg, *The Judicial Role in Trademark Law*, 52 B.C. L. Rev. 1283, 1306 (2011) (“Congress is unlikely to codify a uniform approach to trademark adjudication (beyond the occasional burden allocation), and it is questionable that such an effort could plausibly provide the needed flexibility to anticipate the range of cases that drive the evolution of doctrine.”).

437. FRANK B. CROSS, *THE THEORY AND PRACTICE OF STATUTORY INTERPRETATION* 43 (2008).

438. Grynberg, *supra* note 119, at 1300.

administrative and political costs make the likelihood of legislative action rare.⁴³⁹

Since its earliest days, common law crafted the boundaries of trademark rights.⁴⁴⁰ Thus, despite the LOC factors' questionable effectiveness in implementing trademark law's substantive goals, judicial lawmaking has advanced the trademark system's goals. Setting standards without specifying details can lead to variability, which might be controlled through the approaches this Article discussed. The difficulty of getting diverse people to agree on variability-reducing rules is one reason why standards, and not rules, are put in place. Standards might be the best that such leaders can do. Lawmakers might reach a compromise on a standard (and tolerate the resulting noise) if that is the price of enacting law at all.

Post-enactment, the costs of decisions tend to become impossibly large. The better systemic alternative is to deploy the rules of thumb in Part IV to simplify the application of the law and make it more predictable. Common law can adapt to the nuances of the facts while precedent anchors the body of jurisprudence, giving it coherence in form, if not also in substance. Moreover, deep learning algorithms can curate the relevant datapoints to respond to changing conditions. The task of advancing the trademark system's goals will likely fall on the district and appellate courts. The Supreme Court has never addressed or endorsed a particular test for determining the LOC standard and shows no sign that it intends to do so.⁴⁴¹

Three key factors—actual confusion, mark similarity, and the proximity of goods and services (referred to here as the Troika factors)—help structure the LOC inquiry and gives notice of pertinent issues and relevant evidence and a more solid basis for predicting case outcomes. Similarly, safe harbors for expressive and descriptive uses allow courts to dispose of LOC cases more simply and justly. Using AI to assist judges with determining the LOC of dispute trademarks, this reduces judicial error and it will likely be up to courts, not Congress, to catalyze change.

VI. RULES, STANDARDS, AND SAFE HARBORS

This final Section distills the lessons learned so far and brings the discussion full circle to consider the implications for multifactor tests as legal

439. See Parchomovsky & Stein, *supra* note 383, at 171.

440. See *supra* Part III.

441. The closest it has come was in 1877 where it adopted the likely confusion standard, holding that infringement occurs when “ordinary purchasers” exercising “ordinary caution” are likely to be misled. *McLean v. Fleming*, 96 U.S. 245, 251 (1877). However, the Court did not set forth a test.

vehicles for operationalizing rules and standards more broadly. The discussion is informed by the foregoing discussion on LOC and goes beyond it to make the point that there are transferable lessons to be learned elsewhere and vice versa. Scholars fiercely debate the distinction between rules and standards, including when they apply.⁴⁴² The rules-versus-standards dilemma manifests in society's unsettled tussle between accommodating individualistic and communal goals.⁴⁴³

Rules are generally simpler than standards to understand and are easier for people to plan their conduct. The simplest rules look to a single fact, such as a speed limit, to determine a legal outcome.⁴⁴⁴ Clarity makes plaintiffs less likely to bring vexatious suits since parties see what constitutes a weak claim.⁴⁴⁵ Even if plaintiffs do send these letters, small businesses and individuals receiving cease-and-desist letters from trademark owners can point to simple and clear rules rather without hedging advice in a complex memo filled with what-ifs.⁴⁴⁶ For this reason, criminal laws tend to be rule-based.⁴⁴⁷

To better guide the open-ended analysis, courts over the decades encrusted the LOC standard with up to thirteen factors in some circuits, to make the analysis proceed in a lockstep fashion. For this reason, Beebe observed “multifactor tests appear to be the least worst alternative, if not the only alternative, to a wide open ‘totality of the circumstances’ or ‘rule of reason’

442. Parchomovsky & Stein, *supra* note 383, at 167–68 (“The distinction between rules and standards has preoccupied scholars from different methodological persuasions, spawning a voluminous theoretical literature with many important insights.”); James J. Park, *Rules, Principles, and the Competition to Enforce the Securities Laws*, 100 CALIF. L. REV. 115, 130–43 (2012) (analyzing the rules-versus-standards dichotomy in securities law); James D. Ridgway, *Changing Voices in a Familiar Conversation About Rules vs. Standards: Veterans Law at the Federal Circuit*, 2011, 61 AM. U. L. REV. 1175, 1183–90 (2012) (using the rules-versus-standards framework to analyze Federal Circuit’s decisions on veterans’ rights); Kathleen M. Sullivan, *The Supreme Court, 1991 Term—Foreword: The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 69–83 (1992) (examining Supreme Court Justices’ divisions over rules and standards).

443. See Kennedy, *supra* note 8, at 1766–67 (discussing individualism and altruism).

444. RICHARD A EPSTEIN, SIMPLE RULES FOR A COMPLEX WORLD 24–25 (1995).

445. See Fed. R. Civ. P. 11 (providing penalties).

446. McGeeveran, *supra* note 371, at 2290 (“Risk-averse intermediaries should be more willing to permit an expressive use when they can rely on an unambiguous legal argument in its favor.”).

447. See *Hill v. Colorado*, 530 U.S. 703, 773 (2000) (Kennedy, J., dissenting) (arguing that criminal statute’s “substantial imprecisions will chill speech, so the statute violates the First Amendment”); *Scull v. Virginia ex rel. Comm. on Law Reform & Racial Activities*, 359 U.S. 344, 353 (1959) (“Certainty is all the more essential when vagueness might induce individuals to forego their rights of speech, press, and association for fear of violating an unclear law.”).

type of analysis.”⁴⁴⁸ Unfortunately, the increased decision-making flexibility has led to worse results rather than better ones.⁴⁴⁹

The problem, as we have seen with LOC, is that standards themselves provide little guidance.⁴⁵⁰ Blending the law on trademarks and trade names has also created new triggers for confusion. The Supreme Court rejected a multifactor test for diversity jurisdiction in civil procedure because courts have difficulty processing the factors.⁴⁵¹ Maggie Gardner warned in the context of cross-border disputes that “tests that call for weighing ten or a dozen factors should be viewed skeptically, as judges may be unwilling or even unable to assess all of them independently.”⁴⁵² More broadly, judges have waged an all-out war against multifactor tests characterizing them as a “confession of the inability to devise tests.”⁴⁵³

The unfamiliarity and complexity of the law increases the risk that judges will look for rubrics in the wrong places or simplify factors while searching for a clearer framework. Consider Justice Thomas criticizing multifactor tests for taking a life of their own,⁴⁵⁴ or Justice Stevens criticizing them for generally producing “negative answers,”⁴⁵⁵ or Judge Easterbrook observing that they

448. Beebe, *supra* note 21, at 1649.

449. See Ronald A. Heiner, *The Origin of Predictable Behavior*, 73 AM. ECON. REV. 560, 563, 565 (1983) (positing that “there is greater uncertainty as either an agent’s perceptual abilities become less reliable or the environment becomes more complex” and explaining that “when genuine uncertainty [thus defined] exists, allowing greater flexibility to react to more information or administer a more complex repertoire of actions will not necessarily enhance an agent’s performance”).

450. See John E. Calfee & Richard Craswell, *Some Effects of Uncertainty on Compliance with Legal Standards*, 70 VA. L. REV. 965, 966–67 (1984) (attesting uncertainty associated with standards may chill desirable conduct).

451. *Hertz Corp. v. Friend*, 559 U.S. 77, 92 (2010).

452. Maggie Gardner, *Abstention at the Border*, 105 VA. L. REV. 63, 92 (2019); see also Robert G. Bone, *Who Decides? A Critical Look at Procedural Discretion*, 28 CARDOZO L. REV. 1961, 2016 (2007) (“[T]he resulting process can easily turn into ad hoc weighing that lacks meaningful constraint and jeopardizes principled consistency over the system as a whole.”).

453. Frank H. Easterbrook, *What’s So Special About Judges?*, 61 U. COLO. L. REV. 773, 780 (1990).

454. *Doggett v. United States*, 505 U.S. 647, 670 (1992) (Thomas, J., dissenting) (“But Barker’s factors now appear to have taken on a life of their own. Instead of simply guiding the inquiry whether an individual who has been deprived of a liberty protected by the Clause is entitled to relief, Barker has become a source for new liberties under the Clause.”).

455. *Middlesex Cnty. Sewerage Auth. v. Nat’l Sea Clammers Ass’n*, 453 U.S. 1, 25 (1981) (Stevens, J., concurring in part and dissenting in part) (“[M]ultifactor balancing tests generally tend to produce negative answers.”).

invited judges to “throw a heap of factors on a table and then slice and dice to taste.”⁴⁵⁶

Studies about multifactor tests with real judges in real cases show judges ignore most factors when faced with a long list.⁴⁵⁷ Instead, faced with complex facts and tight deadlines, judges focus on the facets of the case that are most compelling to them.⁴⁵⁸ Gardner points to how, in a procedural context, concrete and immediate facts “like efficiency, delay, docket congestion, gamesmanship, and the short-term interests of sympathetic parties may take precedence,” especially if judges struggle with a poorly fitting framework.⁴⁵⁹ In such instances, courts prioritize addressing the concrete and the familiar, while de-prioritize the unfamiliar and the difficult, leaving those [factors] underapplied.

The problem here is that this “choose your own adventure” approach is, as the Supreme Court pointed out in the context of determining a corporation’s principal place of business, “at war with administrative simplicity.”⁴⁶⁰ In doing so, that approach “has failed to achieve a nationally uniform interpretation of federal law, an unfortunate consequence in a federal legal system.”⁴⁶¹ In trademark law, while courts may lean on mark strength, defendants’ intent, surveys, and consumer sophistication to shape LOC’s contours, it is impossible to know in advance whether a court will find them probative. Salience causes judges to overweigh vivid, concrete foreground information at the expense of abstract, aggregated background information. Factors become a checklist that substitutes judicial analysis and ultimately produces intuitive decisions, “hiding their lack of analytic rigor beneath a veneer of rationality.”⁴⁶²

The risk of wrongly calibrating multifactor tests is a common one.⁴⁶³ So there is the risk of bidirectional coherence-based reasoning whenever judges

456. *Reinsurance Co. of Am., Inc. v. Administratia Asigurarilor de Stat*, 902 F.2d 1275, 1283 (7th Cir. 1990) (Easterbrook, J., concurring).

457. *See, e.g., Beebe, supra* note 21, at 1601 n. 88.

458. *See Guthrie et al., supra* note 314, at 787–816 (summarizing survey results that suggest judges are susceptible to common cognitive shortcuts like anchoring, framing, hindsight bias, egocentric biases, and the representativeness heuristic).

459. Gardner, *supra* note 337, at 964.

460. *Hertz Corp. v. Friend*, 559 U.S. 77, 89 (2010).

461. *Id.* at 92.

462. Andrea M. Hall, *Standing the Test of Time: Likelihood of Confusion in Multi Time Machine v. Amazon*, 31 BERKELEY TECH. L.J. 815, 841 (2016).

463. *See generally* Oona A. Hathaway, *Path Dependence in the Law: The Course and Pattern of Legal Change in a Common Law System*, 86 IOWA L. REV. 601 (2001) (discussing the problem of path dependence in the common law).

must apply more than a few factors. The problem pervades jury verdicts⁴⁶⁴ and social science testimony in the law on evidence.⁴⁶⁵ Critics contend that a multifactor test “permits courts under the guise of a well-reasoned opinion and in the name of equity to strike a ‘balance’ which justifies these courts’ view of the underlying merits of a case.”⁴⁶⁶ For instance, Simon found coherence-based reasoning led criminal juries to assess evidence in a way that makes them more likely to find guilt beyond a reasonable doubt. Further, he argues that “[o]ver time, unsupported variables or those suppressed by other variables degrade and even die out, while those that are mutually supported gain strength.”⁴⁶⁷

There is also the risk that courts will choose which factors to apply based off of precedent, i.e., whether to apply the same factors as in similar cases, despite factual differences and explicit warnings against applying the test inflexibly.⁴⁶⁸ Behavioral psychology suggests that judges distill the law from prior opinions, deferring to precedent because of a professional interest in avoiding conflict with their brethren or minimizing the risk of reversal on appeal.⁴⁶⁹ Avoiding reinventing the wheel also conserves time and effort, particularly when inconvenient precedent is binding or must be distinguished. Thus, in a case involving *forum non conveniens*, even though the applicable test was not meant to be a definitive “catalog” of considerations, judges and litigants have treated those factors have been treated as such ever since.⁴⁷⁰

In sum, the way courts currently apply many multifactor tests makes it difficult to account for relative factor strength, deviate from underlying policy considerations, or clarify what is at stake.⁴⁷¹ Additionally, these tests allow courts to incorporate different or competing policy conceptions in a single malleable analysis. As a result, different courts reach opposite or inconsistent results using similar facts. In practice, parties can generally support opposing

464. See Jennifer K. Robbennolt, John M. Darley & Robert MacCoun, *Symbolism and Incommensurability in Civil Sanctioning: Decision Makers as Goal Managers*, 68 BROOK. L. REV. 1121, 1148–57 (2003).

465. See Maxine D. Goodman, *A Hedgehog on the Witness Stand—What’s the Big Idea?: The Challenges of Using Daubert to Assess Social Science and Nonscientific Testimony*, 59 AM. U. L. REV. 635, 672 (2010).

466. Robert Alpert, *The Export of Trademarked Goods from the United States: The Extraterritorial Reach of the Lanham Act*, 81 TRADEMARK REP. 125, 145 (1991).

467. Simon, *supra* note 43, at 521.

468. Hall, *supra* note 462, at 840.

469. See Stephen M. Bainbridge & G. Mitu Gulati, *How Do Judges Maximize? (The Same Way Everybody Else Does—Boundedly): Rules of Thumb in Securities Fraud Opinions*, 51 EMORY L.J. 83116–17 (2002).

470. Maggie Gardner, *Retiring Forum Non Conveniens*, 92 N.Y.U. L. REV. 390, 419 (2017).

471. Liu, *supra* note 104, at 579 (2008) (“Under a multi-factor balancing test, it is difficult to register the relative strength of the factors.”).

positions on each factor by citing one case or another.⁴⁷² Later cases then perpetuate a chain of decisions overemphasizing these malleable factors.

Any viable solution needs to move the scholarly debate beyond the rules-standards dichotomy to consider a new framework with the certainty that rules will mark out the boundaries of reasonable claims, allowing courts to dispose of clearly unreasonable ones. At the same time, safe harbors protect the core policies most in danger of invasion by trademark expansionism while making it simpler and cheaper for businesses to perform due diligence and comply with the law.⁴⁷³

This Article demonstrates how the Troika of relevant LOC factors and twin safe harbors leverages existing AI deep learning techniques. For example, AI-assisted analysis assigns weights to each factor and considers this weighted range of possibilities. AI also helps mitigate coherence-based reasoning by getting judges to consider the weaknesses in their positions and the merits of the opposition.

How successive courts interpret a “reasonable” speed eventually informs drivers that anything above eighty miles per hour is dangerous, and likewise, the work of courts over time will reveal the point where a “similar” mark becomes discernable. Courts can also identify recurring undesirable behaviors and ban them outright. Then, the algorithm can use those cases as a basis for establishing a more general prohibition on activities falling into the same family or genre. In so doing, AI would create per se rules of illegality and safe harbors that standards cannot while doing so more easily than rules.⁴⁷⁴ The result is a familiar yet concise, precise, and efficient framework for preempting, counseling and adjudicating trademark disputes. The standard thus attains the amphibious benefits of becoming more rule-like while retaining its suppleness.

VII. CONCLUSION

Congress built a degree of indeterminacy into the LOC standard as a feature and not a bug. Over the years, however, the jurisprudential roots of trademark law has become unruly and tangled. Unwanted variability and bias in judgments cause serious problems by including complex and irrelevant factors, including financial loss and rampant unfairness. Meanwhile, simple rules and algorithms have big advantages over human judges.

472. See Grynberg, *supra* note 85, at 116–17.

473. See Isaac Ehrlich & Richard A. Posner, *An Economic Analysis of Legal Rulemaking*, 3 J. LEGAL STUD. 257, 266 (1974).

474. Parchomovsky & Stein, *supra* note 383, at 171 (“No matter how hard legislatures try, they will fail to come up with fully specified rules that accurately represent every possible contingency in all future states of the world.”).

This Article uses empirical studies, case law, and the latest experimental psychology and artificial intelligence literature to shift the debate from critiquing to simplifying the likelihood of confusion standard. It explains how three core factors, combined with two safe harbors and today's deep learning algorithms, would enable courts to reach consistent and accurate results. A simplified framework in trademark law promotes fair play, safeguards expressive uses, and enhances access to justice. This framework, in turn, points to the importance and general applicability of a strategy to reduce bias, variability and noise in judicial decision-making using simplified rules and AI-refined guidelines.

Future work can provide a contemporary empirical analysis of the various LOC factors and how they interact, whether courts “economize” by using the Troika to provide early off-ramps to litigants or “fold” factors within each other to focus on the most relevant ones. Empirical data can also show the most dominant circuit, and whether its dominance impacts the Troika. On the AI side of things, future work can chart how AI optimizes policy performance in analyzing LOC factors without being ossified in outdated, erroneous, or biased data. Conceivably, the algorithm will need to replicate how a human perceives a mark in the marketplace. Developers will also need to deal with issues of bias, accountability, and data scarcity when deploying AI in trademark disputes.

The focus on the multifactor test for the LOC standard in trademark law also provides lessons for other types of multifactor tests. Unwanted variability matters because random errors do not cancel one another out. Likewise, consistently relying on irrelevant factors like intent results in biased decisions. A familiar yet concise, precise, and efficient framework helps preempt, counsel, and adjudicate disputes. In this way, standards can attain the amphibious benefits of becoming more rule-like while retaining their suppleness. Confusion is, in a word, simplified.