

33:1 BERKELEY TECHNOLOGY LAW JOURNAL

2018

Pages

1

to

364

Berkeley Technology Law Journal

Volume 33, Number 1

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

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

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

Copyright © 2018 Regents of the University of California.
All Rights Reserved.



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

BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 33

NUMBER 1

2018

TABLE OF CONTENTS

ARTICLES

INFORMATION FIDUCIARIES IN PRACTICE: DATA PRIVACY AND USER EXPECTATIONS	1
<i>Ariel Dobkin</i>	
COMPUTER-AIDED DESTRUCTION: REGULATING 3D-PRINTED FIREARMS WITHOUT INFRINGING ON INDIVIDUAL LIBERTIES	51
<i>Jessica Berkowitz</i>	
IP PRIVATEERING IN THE MARKETS FOR DESKTOP AND MOBILE OPERATING SYSTEMS	85
<i>Daniel L. Rubinfeld</i>	
AT THE PRIVACY VANGUARD: CALIFORNIA'S ELECTRONIC COMMUNICATIONS PRIVACY ACT (CALECPA)	131
<i>Susan Freiwald</i>	
DIGITAL EXHAUSTION: NEW LAW FROM THE OLD WORLD.....	177
<i>Lothar Determann</i>	
PATENT POOL OUTSIDERS	225
<i>Michael Mattioli</i>	
THE RIGHT TOOLS: EUROPE'S INTERMEDIARY LIABILITY LAWS AND THE EU 2016 GENERAL DATA PROTECTION REGULATION.....	287
<i>Daphne Keller</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 (Boalt Hall) 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 33 BERKELEY TECH. L.J. ____ (2018).

BTLJ ONLINE

The full text and abstracts of many previously published *Berkeley Technology Law Journal* articles can be found at <http://www.btlj.org>. Our site also contains a cumulative index; general information about the *Journal*; 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 the ExpressO 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 ExpressO submission website can be found at <http://law.bepress.com/expresso>.

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

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

DONORS

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

Partners

COOLEY LLP

HOGAN LOVELLS

FENWICK & WEST LLP

ORRICK, HERRINGTON &
SUTCLIFFE LLP

WHITE & CASE LLP

Benefactors

COVINGTON & BURLING LLP

MORRISON & FOERSTER LLP

FISH & RICHARDSON P.C.

SIDLEY AUSTIN LLP

JONES DAY

WEIL, GOTSHAL & MANGES LLP

KIRKLAND & ELLIS LLP

WILMER CUTLER PICKERING HALE
AND DORR LLP

LATHAM & WATKINS LLP

WILSON SONSINI GOODRICH &
ROSATI

MCDERMOTT WILL & EMERY

WINSTON & STRAWN LLP

Corporate Benefactors

BLOOMBERG LAW	LITINOMICS
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION	MICROSOFT CORPORATION
CORNERSTONE RESEARCH	MOZILLA
FUTURE OF PRIVACY FORUM	NERA ECONOMIC CONSULTING
GOOGLE, INC.	NOKIA
HEWLETT FOUNDATION, THROUGH THE CENTER FOR LONG-TERM CYBERSECURITY	PALANTIR
INTEL	RLM TRIALGRAPHIX
INVENTIONSHARE	THE WALT DISNEY COMPANY

Members

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

BOARD OF EDITORS

2017–2018

Executive Committee

<i>Editor-in-Chief</i> CHRISTIAN CHESSMAN	<i>Senior Articles Editors</i> ALICE CHI JON MADDERN ROBERT OLSEN	<i>Senior Executive Editor</i> TAMARA WIESEBRON <i>Senior Production Editor</i> KRISTOFER HATCH
<i>Managing Editor</i> DUSTIN VANDENBERG		
<i>Senior Scholarship Editor</i> JOE CRAIG	<i>Senior Annual Review Editors</i> VANESSA ING JOYCE LI	<i>Senior Online Content Editor</i> CHANTE WESTMORELAND

Editorial Board

<i>Submissions Editors</i> CHRISTOPHER BROWN AMIT ELAZARI	<i>Production Editors</i> LOUISE DECOPPET SAFFA KHAN MEGAN MCKNELLY CHELSEA MORI	<i>Technical Editors</i> NADIA KALE DANIEL LUECKE AYN WOODWARD
<i>Annual Review Editors</i> MARIA BELTRAN NIR MAOZ	<i>Notes & Comments Editors</i> BRITTANY JOHNSON ANDREW NGUYEN	<i>Symposium Editors</i> DARIUS DEHGHAN JESSICA HOLLIS
<i>Web & Technology Editors</i> JOHN HAZELWOOD TED KANG	<i>Online Content Editor</i> KATIE BURKHART <i>Podcast Editor</i> ANTHONY BEDEL	<i>LLM Member Relations Editors</i> JONATHAN DEBBI MARTYNA SKRODZKA
<i>Member Relations Editor</i> BARCLAY OUDERSLUYS	<i>Alumni Relations Editor</i> ERICA SUN	<i>External Relations Editor</i> BLAKE MEREDITH
	<i>Articles Editors</i>	
TIANA BAHERI ALEX BARATA BRANDON CHAVEZ CHRIS CHUANG ERIC CHUANG	KATHARINE CUMMINGS MARK JAYCOX YARDEN KAKON LAURA KELLEY AARON LEE DINA LJEKPERIC	ANGELA LYONS-JUSTUS CHARLES MILLER BIHTER OZEDIRNE AAMIR VIRANI ELLE WANG

MEMBERSHIP

Vol. 33 No. 1

Associate Editors

LORRAINE ABDULHAD	KATIE GONZALEZ	PAYMANEH PARHAMI
NIYATI AHUJA	ELIZA GREEN	SANJANA PARIKH
ROBERTA AMORIM	ANUSHREE GUPTA	ANJELI PATEL
BLAKE ANDERSON	KAREN GRAEFIN VOM HAGEN	AYESHA RASHEED
CHELSEA ANDRE	MICHAEL HOMER	COLIN RAVELLE
NICHOLAS CALCATERRA	JONATHAN HUANG	COURTNEY REED
SAVANNAH CARNES	VICTORIA HUANG	NOELLE REYES
STELLA CHANG	CAROLINA JUVIN	ALYSE RITVO
DANIEL CHASE	ALEXANDER KROIS	AYELET ROSENTAL
INAYAT CHAUDHRY	HYUN KYU LEE	ELIZABETH FREEMAN ROSENZWEIG
GILBERT CHOI	YUAN LI	MIRANDA RUTHERFORD
RIYANKA ROY CHAUDHURY	JULIA LIPIZ	ARPITA SENGUPTA
NOMI CONWAY	DENISE LOUZANO	KELLY SERANKO
HUGO CUGNET	SAM MILLER	AISLINN SMALLING
TRENTON DAVIS	ARUNDHATI NAYUDU	WESLEY TIU
JOHN DETERDING	KATHERINE NOLAN	MEI XUAN
GRACE FERNANDEZ	DEBBIE OH	FAN YANG
YESENIA FLORES	LARA OLAFSDOTTIR	LI ZHANG
SREYA GANGULY		EVAN ZIMMERMAN

Members

DIANE AGUIRRE-DOMINGUEZ	CHANTE ELIASZADEH	PING LIU
ANANDITA ARORA	JORDAN FRABONI	SABRINA MCGRAW
LUKE BLACKETT	CHRIS GAO	FEI MO
NICHOLAS BOLDUC	YESOL HAN	CRISTINA MORA
LAUREN CARROLL	SPENCER HAZAN	SAISHRUTI MUTNEJA
CAROLINE YEN-RON CHEN	MEHTAB KHAN	SADAF NAKHAEI
SIYING CHEN	SINDHU KOMMI	SILVIA SEGADE
CONCORD CHEUNG	RYAN KWOCK	EMRE YUZAK
		TIANYUAN ZHUANG

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
U.C. Berkeley School of Law

MATTHEW D. POWERS
Tensegrity Law Group, LLP

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

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

REGIS MCKENNA
Chairman and CEO
Regis McKenna, Inc.

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

PETER S. MENELL
*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 2017–2018

Executive Director

JIM DEMPSEY

Faculty Directors

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

Fellows

KATHRYN HASHIMOTO	JOSHUA KROLL
GRAHAM RAVDIN	

Staff Directors

JANN DUDLEY	IRYS SCHENKER
RICHARD FISK	CLAIRE TRIAS

INFORMATION FIDUCIARIES IN PRACTICE: DATA PRIVACY AND USER EXPECTATIONS

Ariel Dobkin[†]

ABSTRACT

Every day, consumers give their personal information to corporations in exchange for free or inexpensive services. As service providers collect increasingly personal information, they will not be able to use it just to inform business decisions, but also to manipulate users, push agendas, or discriminate surreptitiously. And users may not know exactly how these companies collect and use their data, so they may not be equipped to respond effectively to objectionable data collection practices. The law does nothing to manage this relationship, and in fact, the Supreme Court has interpreted the First Amendment to prevent certain regulation of data collection or usage. However, imposing an information fiduciary duty on service providers could ensure that they use data only in ways that are consistent with users' expectations. This Article maintains that service providers should be proscribed from utilizing users' personal information to manipulate them and discriminate against them, and that firms should be prohibited from sharing data with third parties under certain circumstances. It also proposes that firms engage with their users by employing easy-to-understand privacy policies that help reduce information asymmetries. Ultimately, imposing an information fiduciary duty on service providers can ensure that firms are able to grow and innovate and that their users—whose data is necessary for that growth—are protected as well.

DOI: <https://doi.org/10.15779/Z38G44HQ81>

© 2018 Ariel Dobkin.

[†] Yale Law School, J.D. 2017. The author would like to thank Jack Balkin for his thoughtful suggestions and support throughout many stages of this Article. She also thanks James Durling, Jackie Koo, Hilary Ledwell, Jenna Pavelec, Alexandra Perloff-Giles, and Jacobus van der Ven for their invaluable input at various phases of this Article's production. Finally, the author is grateful to Bihter Ozedirne, Charles Miller, and Alice Chi, as well as Christian Chessman and the editors at the *Berkeley Technology Law Journal*, for their careful editing and hard work on this Article.

TABLE OF CONTENTS

I.	INTRODUCTION.....	3
II.	BACKGROUND	8
	A. EXISTING PRIVACY REGIMES.....	8
	B. AN INFORMATION FIDUCIARY DUTY.....	10
	C. HOW FOUR COMPANIES UTILIZE USER DATA.....	12
	1. <i>Walmart</i>	12
	2. <i>Uber</i>	14
	3. <i>Facebook & Google</i>	15
III.	BREACHING FIDUCIARY STATUS: FOUR MAIN PRINCIPLES	17
	A. ANTI-MANIPULATION OF THE USER.....	18
	1. <i>A Dignity- and Autonomy-Focused Conception of Manipulation</i>	19
	2. <i>A Welfarist Conception of Manipulation</i>	19
	3. <i>Targeted Advertising</i>	20
	4. <i>Hypotheticals</i>	21
	B. ANTIDISCRIMINATION.....	26
	1. <i>Access to Services</i>	27
	2. <i>Price Discrimination</i>	29
	3. <i>Digital Redlining</i>	30
	4. <i>Hypotheticals</i>	32
	C. LIMITED SHARING WITH THIRD PARTIES.....	36
	1. <i>Identities and Obligations of Third Parties</i>	37
	2. <i>Hypotheticals</i>	41
	D. VIOLATING THE COMPANY'S OWN PRIVACY POLICY.....	43
	1. <i>An Information Fiduciary's Privacy Policy</i>	45
	2. <i>Hypothetical: Facebook Pushes a Political Agenda, Part II</i>	46
IV.	ENFORCING THE INFORMATION FIDUCIARY DUTY.....	47
V.	CONCLUSION	49

“It’s the little things that reveal what a company is all about at its core. . . . A great, long-lived brand begins and ends with trust.”

—Peter Sims, whose data was displayed publicly at an Uber launch party¹

I. INTRODUCTION

Imagine riding in an Uber car and receiving a phone call from a friend in another city. When you pick up, she recites your location to you. When you turn a corner, she knows where you are. When you have arrived at your destination, she knows that too. Or imagine being a girl in high school and your father finding out you are pregnant because Target sent you coupons for maternity clothes. Or feeling more depressed over the last week, only to find out that over the same time period, Facebook performed an experiment to tinker with its users’ emotions.

Real people have found themselves in each of these situations over the past several years. Peter Sims, an entrepreneur in New York, found himself in the first situation in 2014, when Uber displayed his location on a wall at its Chicago launch party.² A young girl in Minneapolis found herself in the second situation several years earlier.³ And Facebook did in fact perform an experiment to “manipulate[] the news feeds of over half a million randomly selected users to change the number of positive and negative posts they saw, [as] part of a psychological study to examine how emotions can be spread on social media.”⁴ In each situation, a company took advantage of personal information it possessed—information with which users had entrusted them—for its own benefit. The service providers used that data in a way that likely breached the trust that Peter Sims, the young girl, and half a million others had placed in them. In none of these situations, fortunately, did a report of harm surface, but the potential was not far off. Imagine if Mr. Sims had a dangerous stalker, if the Minneapolis teenager had an abusive parent, or if a depressed Facebook user had been pushed far enough to commit suicide. The

1. Peter Sims, *Can We Trust Uber?*, SILICON GUILD (Sept. 26, 2014), <https://thoughts.siliconguild.com/can-we-trust-uber-c0e793deda36> [https://perma.cc/L7JB-GTDY].

2. *Id.*

3. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/R3D6-HSLN].

4. Vindu Goel, *Facebook Tinkers with Users’ Emotions in News Feed Experiment, Stirring Outcry*, N.Y. TIMES (June 29, 2014), www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html [https://perma.cc/CL49-GNWK].

companies' efforts to boost their profits took precedence over protecting the sensitive and private information of their users.

Every day, users knowingly and unknowingly trade their data—often instead of their money—for goods and services with companies that profit off of their personal information.⁵ In fact, at least 77.4% of websites globally track visitors' data.⁶ Users may on some level realize that their data is valuable, but they may not think twice before handing it over to service providers; those who do consider it may still prefer paying with data to paying with money.⁷ This behavior by both groups of people is a manifestation of their trust in these companies. Even as users may be unable to articulate exactly how service providers should and should not use their data, they have implicit expectations. We each have a gut reaction that tells us when a company has crossed the line: we may have no problem when Uber remembers our home address so that we can avoid typing it in every time we use the service, but we would feel that our privacy had been violated if Uber were to provide a database through which anyone could look up our rider histories. Few people mind that Facebook shows them targeted advertisements,⁸ but many might react negatively if Facebook began selling access to their Facebook profiles to potential employers or landlords. Users' expectations and tolerance differ at the margins,

5. See ANNA BERNASEK & D.T. MONGAN, ALL YOU CAN PAY: HOW COMPANIES USE OUR DATA TO EMPTY OUR WALLETS 208 (2015); see also David B. Kline, *How Does Google Make Money? Ads, Ads, Ads*, MOTLEY FOOL (June 14, 2015, 11:31 AM), <https://www.fool.com/investing/general/2015/06/14/how-does-google-make-money-ads-ads-ads.aspx> [<https://perma.cc/UX7Y-REA8>] (explaining that 90% of Google's revenue in 2015 came from advertising); Tim Wu, *Facebook Should Pay All of Us*, NEW YORKER (Aug. 14, 2015), <http://www.newyorker.com/business/currency/facebook-should-pay-all-of-us> [<https://perma.cc/N5JH-8YBL>] (“The two-hundred-and-seventy-billion-dollar valuation of Facebook, which made a profit of three billion dollars [in 2014], is based on some faith that piling up all of that data has value in and of itself. It’s like a virtual Fort Knox—with a gold mine attached to it.”).

6. Sam Macbeth, *Tracking the Trackers: Analysing the Global Tracking Landscape with GhostRank*, GHOSTERY (July 2017), <https://www.ghostery.com/lp/study> [<https://perma.cc/27EC-R5J8>] (describing a study of 850,000 users and 144 million page loads in more than twelve countries).

7. The Digital Advertising Alliance, for example, found that 58% of adults who download phone apps “preferred free, ad-supported apps to those that required some form of payment” Greg Sterling, *Survey: 58 Percent Prefer Ad-Based Apps to Paid, Freemium Models*, MARKETING LAND (Oct. 26, 2014, 11:31 AM), <http://marketingland.com/survey-proclaims-consumer-preference-ad-supported-apps-daa-readies-mobile-appchoices-105463> [<https://perma.cc/V9LN-KXAZ>].

8. David Kirkpatrick, *Study: 71% of Consumers Prefer Personalized Ads*, MARKETING DIVE (May 9, 2016), <http://www.marketingdive.com/news/study-71-of-consumers-prefer-personalized-ads/418831> [<https://perma.cc/K3RA-MTBG>].

but certain practices would likely be widely regarded as having crossed a line. And it is important for service providers to maintain users' trust, which "can evaporate in an instant if customers feel their data is being used improperly, or not effectively protected."⁹

But the threat of trust disappearing is not enough to influence service providers to protect user privacy on their own. Because users often do not know or understand how their data is being used, the market cannot simply "work its magic" and encourage best privacy practices; markets rely on consumers having enough knowledge to inform their decision-making.¹⁰ When consumers lack information, they cannot respond to company practices effectively enough to affect the market. And thus, too often, companies are able to cross the line into data usages many users would oppose, because the users never know about it.¹¹

Companies readily acknowledge that they are not transparent about their data usage. In January 2016, *The Economist's* Intelligence Unit released the results of a study demonstrating that almost sixty percent of professionals surveyed globally are "generating revenue from the data they own and will continue to do so," and eighty-three percent say it makes "existing products or services more profitable."¹² But only thirty-four percent of those surveyed believe that "their firms are 'very effective' at being transparent with customers about how they use their data," while nine percent "admit to being 'somewhat' or 'totally ineffective.'"¹³ Despite this admitted lack of transparency, the U.S. government does not adequately regulate service providers in any comprehensive way.

9. Bernard Marr, *Big Data Facts: How Many Companies Are Really Making Money from Their Data?*, FORBES (Jan. 13, 2016, 2:24 AM), www.forbes.com/sites/bernardmarr/2016/01/13/big-data-60-of-companies-are-making-money-from-it-are-you/ [<https://perma.cc/NNC7-8642>].

10. See Ryan Bubb & Richard H. Pildes, *How Behavioral Economics Trims Its Sails and Why*, 127 HARV. L. REV. 1593, 1601, 1639 (2014) (discussing information asymmetry as a reason for market failure); Brendan A. Cappiello, *The Price of Inequality and the 2005 Bankruptcy Abuse Prevention and Consumer Protection Act*, 17 N.C. BANKING INST. 401, 429 (2013) ("[M]arkets, especially financial markets, require the buyer and seller to have similar knowledge about the transaction in order for it to function properly."); Justin M. Ross, *What Should Policy Makers Know When Economists Say 'Market' Failure?*, 14 GEO. PUB. POL'Y REV. 27, 28 (2009) (noting that "information problems" are a "common source" of market failure).

11. See, e.g., *supra* notes 2–4 and accompanying text.

12. *The Business of Data*, ECONOMIST 7, 10 (2015), www.eiuperspectives.economist.com/sites/default/files/Business%20of%20Data%20briefing%20paper%20WEB.pdf [<https://perma.cc/ERN9-U8CX>]; see also Marr, *supra* note 9.

13. ECONOMIST, *supra* note 12, at 4, 12.

Companies are committed to keeping it that way. Walmart, for example, spent almost \$34 million on lobbying over five years “on some variation of ‘privacy, online advertising and data protection,’ ‘privacy and online behavioral advertising legislation,’ or ‘privacy issues related to e-commerce.’”¹⁴ And that was during a period in which Congress was not pushing to regulate data collection in the first place. The laws that currently exist to protect individuals’ data focus on specific subject matters or populations, rather than establishing a minimum level of protection across the board. For instance, federal laws exist to protect children’s data¹⁵ and to regulate data usage in particular fields.¹⁶ Additionally, federal agencies have sued companies for violating their own privacy policies.¹⁷ The Obama Administration published white papers on data privacy that recognized the need for better protections, but it never suggested a comprehensive solution.¹⁸

More problematically, a 2011 Supreme Court decision, *Sorrell v. IMS Health*,¹⁹ indicates that in at least some circumstances, the First Amendment protects the sale of data by private firms. There, the Court struck down a Vermont statute restricting the sale, transmission, or use of pharmaceutical data, after subjecting it to heightened scrutiny.²⁰ This decision complicated the possibility of data privacy regulation by bringing at least some data sharing within the protection of the First Amendment.

Thus, the current state of the law not only fails to protect the average user, but also indicates that regulating the way data is used or shared may be unconstitutional under the First Amendment. The government can certainly regulate little pockets that may withstand heightened scrutiny, but absent some

14. CTR. FOR MEDIA JUSTICE ET AL., CONSUMERS, BIG DATA, AND ONLINE TRACKING IN THE RETAIL INDUSTRY: A CASE STUDY OF WALMART 14 (2013), http://centerformediajustice.org/wp-content/uploads/2014/06/WALMART_PRIVACY_.pdf [<https://perma.cc/7UVT-MWPQ>].

15. *See, e.g.*, Children’s Online Privacy Protection Rule, 16 C.F.R. pt. 312 (2013).

16. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; Truth in Lending Act, 15 U.S.C. § 1601 (2012).

17. *See, e.g.*, *Privacy & Data Security Update (2015)*, FED. TRADE COMM’N (Jan. 2016), www.ftc.gov/reports/privacy-data-security-update-2015 [<https://perma.cc/ZW9S-ZBYN>] (summarizing FTC enforcement actions including “over 130 spam and spyware cases and more than 50 general privacy lawsuits”).

18. *See, e.g.*, WHITE HOUSE, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf [<https://perma.cc/ZY36-LXFY>] (calling attention to the importance of data privacy without proposing any concrete paths forward).

19. 564 U.S. 552, 557 (2011).

20. *Id.*

countervailing theory, the United States is currently unable to grapple with the challenges that lie ahead. While defending freedom of speech is vital, so is protecting consumers' privacy during a time in which companies know more about us than users' friends or families might. The use of personal information by private firms—to advertise, to build artificial intelligence, to shape public opinion, and more—presents incredible opportunities and benefits to society, as well as disturbing possibilities for manipulation and discrimination. In order to manage these challenges, it is necessary to find a way to protect users without interfering with service providers' First Amendment rights.

Conceiving of service providers as “information fiduciaries” may be the way to balance freedom of speech with data privacy, while still allowing service providers to grow and innovate. As designated information fiduciaries, service providers would have “special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute.”²¹ Jack Balkin explains that “in the digital age, because we trust them with sensitive information, certain types of online service providers take on fiduciary responsibilities.”²² In his article, Balkin suggests imposing a general fiduciary duty on service providers who collect or use data, and he reconciles the First Amendment concerns espoused in *Sorrell* with the public's need for increased regulation of data collection and usage by companies.²³ The article argues convincingly for an information fiduciary duty in theory, but the next step is to determine what that duty will look like in practice.

Thus, this Article extends that work by attempting to determine where the line is—what are the things that consumers, as a collective, trust companies *not* to do, and with what practices *are* consumers comfortable? How can policymakers develop an information fiduciary duty that is in line with users' expectations? Ultimately, this Article argues that companies breach the fiduciary duty when they abuse users' trust by: (1) using their data to manipulate them; (2) using their data to discriminate against them; (3) sharing their data with third parties without consent; or (4) violating their own privacy policies. After describing each principle in theory, this Article presents a set of hypotheticals to make the implications of each more concrete. By examining how various fact patterns would interact with the fiduciary duty for the service provider in question, this Article begins to visualize the duty in a way that makes it a practical legal possibility. In these hypotheticals—many of which are inspired by true events—this Article utilizes a set of companies to

21. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016).

22. *Id.* at 1221.

23. The First Amendment is less likely to tolerate the sharing of information about a person to whom you owe a duty of trust and confidence with respect to that information.

determine how an information fiduciary standard might be applied in practice: Walmart, Uber, Facebook, and Google. Although the information fiduciary framework will allow many companies to continue their current practices involving data collection, retention, or usage, the hope is that it will simultaneously prevent unexpected and abusive practices. Finally, the Article closes with a short discussion of what would be necessary to make the information fiduciary duty a legal reality.

II. BACKGROUND

Because this theory—and indeed, this field—is so new, this first Part aims to provide necessary background information, laying the groundwork for a theoretical information fiduciary duty. It first briefly outlines various privacy regimes that do exist and explains their failure to adequately protect the average user’s privacy. Then, it summarizes Jack Balkin’s proposal for an informational fiduciary duty, which, with the proper contours, may be able to fill this gap. Finally, this Part describes the data collection practices of four well-known companies to illustrate common data collection and usage capabilities.

A. EXISTING PRIVACY REGIMES

American law sparsely regulates the ways in which private firms collect and utilize users’ data. The categories of regulation fall into two camps: (1) laws that protect privacy for certain groups of people or certain kinds of data, and (2) enforcement actions by the Federal Trade Commission (FTC) and other agencies as they apply relatively broad mandates to Big Data and its ramifications.²⁴ Although these mechanisms are certainly better than nothing, they allow the typical service provider to utilize data in many objectionable ways. They are inadequate protections on their own.

The United States Congress has passed several statutes regulating data usage.²⁵ However, there is no sweeping standard for how private firms treat data; each law is tied to a specific subject area or protects a certain class of citizens. For example, the Health Insurance Portability and Accountability Act (HIPAA) regulates how healthcare organizations must secure electronic

24. Of course, there are other laws that regulate the way the United States government can collect and use its citizens’ data. Those laws—and their adequacy—are outside the scope of this Article. Similarly, the United States-European Privacy Shield affects how U.S. businesses can interact with the data of European citizens, but because it does not protect American users, it is similarly outside the scope of this Article.

25. *See, e.g.*, Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-6 (2012); Children’s Online Privacy and Protection Rule, 16 C.F.R. pt. 312 (2013).

medical records and, thus, patients' privacy.²⁶ Although it protects all users, it covers only their health data. On the other hand, the Children's Online Privacy and Protection Rule (COPPA), a regulation promulgated by the FTC, covers many categories of data but protects only users under the age of thirteen.²⁷ Congress has not yet attempted to establish a general data regime that regulates private firms in this space.

At present, the only protection users have is the privacy policies that service providers design and implement themselves, and there is no baseline protection to fall back on if they withdraw or weaken these policies. But at least the FTC and other agencies do have the power to hold companies to their own promises. Through enforcement and the threat of enforcement, the FTC ensures firms do not utilize "unfair" or "deceptive" practices, and it has sought consent decrees against service providers who violate their own privacy policies.²⁸ For example, in June 2016, the FTC fined an advertising company \$950,000 for violating its own privacy policy. The company represented to users that it "would only track consumers' locations when they opted in and in a manner consistent with their device's privacy settings."²⁹ In fact, however, InMobi tracked hundreds of millions of users' geolocation data without their consent, even when they had turned off location tracking on their phones.³⁰ Similarly, the Consumer Financial Protection Bureau (CFPB), which is charged with preventing deceptive, unfair, and abusive practices in the consumer financial services space,³¹ fined an online payment platform \$100,000 for advertising that its security protection exceeded industry standards while the "data security practices in fact fell far short of its claims."³²

But enforcing companies' own standards is not enough. Firms should not be able to dictate the standards to which they hold themselves—and regulators would not have power over a company that violates its users' privacy unless it

26. 42 U.S.C. § 1320d-6 (2012); *see also Notice of Privacy Practices*, U.S. DEP'T HEALTH & HUMAN SERVS. (June 16, 2017), <https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html> [<https://perma.cc/K399-2EP7>].

27. 16 C.F.R. §§ 312.2–12.3 (2017).

28. *See* 15 U.S.C. § 45 (2012).

29. Press Release, Fed. Trade Comm'n, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22, 2016), <https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked> [<https://perma.cc/E2D3-UP4J>].

30. *Id.*

31. 12 U.S.C. § 5531 (2012).

32. Press Release, Consumer Fin. Prot. Bureau, CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices (Mar. 2, 2016), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices> [<https://perma.cc/9UDU-K9NX>].

also violated its own policy. That means service providers have an easy out: implement a very broad privacy policy that it is difficult to violate. As the next Section explains, an information fiduciary duty would require a minimum level of protection regardless of the privacy promises companies make on their own.

B. AN INFORMATION FIDUCIARY DUTY

Definitions of a fiduciary vary, but it has been described by one court as:

[T]he acting of one person for another; the having and the exercising of influence over one person by another; the reposing of confidence by one person in another; the dominance of one person by another; the inequality of the parties; and the dependence of one person upon another. In addition, courts have considered . . . knowledge of the facts involved or other conditions giving to one an advantage over the other.³³

As the American Bar Association (ABA) states, “[w]henver one party places trust and confidence in a second person with that second person’s knowledge, it is possible that a fiduciary relationship is created.”³⁴ In other words, fiduciary law “assume[s] that professionals and their clients do not stand on an equal footing.”³⁵ As a result, a fiduciary has a legal obligation to act in the best interests of her clients because the clients depend on the fiduciary.³⁶ This dynamic exists in various industries in many forms. For example, physicians must act in their patients’ best interests and attorneys must act in their clients’ best interests.³⁷ All of these relationships have a common dynamic: there is an information asymmetry, so both parties know that the person with less information will trust or rely on the person with more information. To manage this dependency, the law imposes a special duty on the person with more information to ensure that she does not take advantage of the asymmetry.

Jack Balkin argues that service providers who collect and utilize user data are fiduciaries “in the digital age, because we trust [service providers] with

33. Robert A. Kutcher, *Breach of Fiduciary Duties*, in BUSINESS TORTS LITIGATION 1, 3 (David A. Soley, Robert Y. Gwin & Ann E. Georgehead eds., 2d ed. 2005) (quoting *First Bank of Wakeeney v. Moden*, 681 P.2d 11, 13 (Kan. 1984)).

34. *Id.*

35. Balkin, *supra* note 21, at 1216.

36. *See* Kutcher, *supra* note 33, at 3. A related idea exists in contract law, which protects buyers who rely on a seller’s special expertise through an implied warranty of fitness for a particular purpose. U.C.C. § 2-315 (AM. LAW INST. & UNIF. LAW COMM’N 2012).

37. While not all of these relationships are known as “fiduciary” relationships, the dynamic itself exists within all of them. The author uses the term “fiduciary” for ease of understanding.

sensitive information.”³⁸ As he explains, end-users are vulnerable to these companies but dependent on them, while service providers are experts on their own data collection and usage practices. And because of this, “information fiduciaries have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute.”³⁹

This is a point with enormous consequences: because users trust service providers with their information, the law should impose a duty to protect the users. But agreeing that providers owe a “fiduciary duty” is only the first step. The next move is to determine what the duty looks like: which practices may service providers implement consistent with their duty, and which must they avoid? In listing the “literally hundreds of ways in which [general] fiduciaries may breach [their] duties,” the ABA includes failure to act in another’s best interest, misuse of confidential information, misuse of superior knowledge or position, failure to disclose, and misappropriation of property.⁴⁰ All of these breaches stem from an understanding that when two parties engage in a fiduciary relationship, the inferior party gives the superior party power to help it make decisions, and thus trusts it to do so in a way that does not harm the inferior party.

The trust users place in service providers “impl[ies] an expectation of predictability.”⁴¹ Users trust businesses with their data and that trust may be broken when companies use it in a way that users could not have predicted. Put another way, when users’ expectations are disregarded by service providers, their trust may be violated. But of course, the confidence people have in a firm they trust often “outstrips [their] knowledge” of what that firm actually does.⁴² So users often misplace their trust and subject themselves to wholly unexpected consequences. But from a market perspective, it is vital for a business to maintain its customers’ trust. In the online space, for example, studies have shown that “consumers prefer to do business with Web sites that

38. Balkin, *supra* note 21, at 1221.

39. *Id.* at 1186. Furthermore, this point addresses the concern that when service providers use or sell data, they are engaging in activity protected by the First Amendment. While the Supreme Court has held that a statute banning the sale, transmission, or use of data by pharmacies, health insurers, and similar entities is an unconstitutional restriction of their right to free speech, *see Sorrell v. IMS Health*, 564 U.S. 552 (2011), imposing an informational fiduciary standard on service providers circumvents this problem. Because a fiduciary relationship has an elevated status, the service provider would have less freedom under the First Amendment than other speakers. Balkin, *supra* note 21, at 1209.

40. Kutcher, *supra* note 33, at 11.

41. ROBERT C. SOLOMON & FERNANDO FLORES, *BUILDING TRUST: IN BUSINESS, POLITICS, RELATIONSHIPS, AND LIFE* 71 (2001).

42. *Id.*

they perceive to be reliable, honest, consistent, competent, fair, responsible, helpful, and altruistic—key components of trust.”⁴³

But *how* do users trust companies to protect their data, and what uses of their data would they oppose if they knew about it? What can users reasonably expect, and what practices would be unpredictable and inconsistent with the duty? Balkin provides a number of general principles to define the information fiduciary duty, such as the idea that a company is an information fiduciary “when the affected individuals reasonably believe that [it] will not disclose or misuse their personal information based on existing social norms of reasonable behavior, existing patterns of practice, or other objective factors that reasonably justify their trust.”⁴⁴ More detail is needed to visualize the information fiduciary duty as something that can be implemented in practice.

C. HOW FOUR COMPANIES UTILIZE USER DATA

In order to understand what users can reasonably expect from service providers, it is helpful to be aware of firms’ capabilities. This Section briefly describes the data capabilities of four companies: Walmart, Uber, Facebook, and Google. These firms serve as the basis for many of this Article’s hypotheticals.⁴⁵ Each company has a meaningful amount of public information about its data practices, sometimes through its own doing and other times through the work of investigative journalists and others. Each also serves as a representative of its broader industry.

1. Walmart

Every hour, Walmart takes in two and a half petabytes—the equivalent of 167 times the books in the Library of Congress—of “unstructured data” from one million customers.⁴⁶ This data covers 145 million Americans, or more than sixty percent of American adults.⁴⁷ Walmart and other big-box stores have access to consumer data including names, contact information (email addresses, physical addresses, and phone numbers), and purchase histories.

43. Miriam J. Metzger, *Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce*, 9 J. COMPUTER-MEDIATED COMM. 00 (2004).

44. Balkin, *supra* note 21, at 1224.

45. This Article deliberately avoids service providers in the health or financial industries. While these areas certainly present a host of important privacy questions, they are already subject to a number of regulations that could distract from a pure analysis of information fiduciary duties.

46. *How Big Data Analysis Helped Increase Walmarks Sales Turnover?*, DEZYRE (Nov. 10 2017), <https://www.dezyre.com/article/how-big-data-analysis-helped-increase-walmarks-sales-turnover/109> [<https://perma.cc/XGV4-XAVS>].

47. *Id.*; see also CTR. FOR MEDIA JUSTICE ET AL., *supra* note 14, at 2.

Based on this, they can often extrapolate (or purchase from a data aggregator) an individual's age, gender, sexual orientation, race, career, income bracket, marital status, parenthood status, and much more.⁴⁸ They can also determine aggregate trends, such as buying patterns by time of year or demographic. Further, the company collects Social Security and driver's license numbers in a number of scenarios, such as when someone cashes a payroll check at a Walmart location.⁴⁹

Users interact with Walmart in brick-and-mortar stores as well as through its website and mobile app. They consciously provide certain data points, such as their addresses and phone numbers when purchasing items online. In these cases, users physically input their data on the screen. In other instances, though, they may not be aware of the types of data the company can collect, such as customers' movements through a store, which can be tracked using cameras, GPS, Wi-Fi, or cellular triangulation.⁵⁰ Even if they are conscious of it, they may not have a choice—in many cases, Walmart is an easy and relatively inexpensive place to purchase necessities and access banking-like services.⁵¹

Walmart's data collection is an attempt to serve customers better, in one sense. The company wants to “optimize the shopping experience for customers when they are in a Walmart store, or browsing the Walmart website or browsing through mobile devices when they are in motion.”⁵² It is trying to anticipate the needs of its customers so that it can always have the right products stocked. It is also attempting to discover how best to push products that consumers might not otherwise buy. Using data mining techniques, Walmart can discover point-of-sale patterns in consumer behavior to provide

48. CJ Frogozo & Kayla Keller, *New Report: Walmart Gathering 'Big Data' That Can Be Used to Invade Privacy, Fuel Hidden Discrimination*, COLOR CHANGE (Nov. 27, 2013), <https://colorofchange.org/press/2013/11/27/new-report-walmart-gathering-big-data-can-be-used/> [https://perma.cc/65BN-WTPM].

49. Constance L. Hays, *What Wal-Mart Knows About Customers' Habits*, N.Y. TIMES (Nov. 14, 2004), <http://www.nytimes.com/2004/11/14/business/yourmoney/what-walmart-knows-about-customers-habits.html> [https://perma.cc/Z6LN-27GK].

50. See Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July 14, 2013), <http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html> [https://perma.cc/A4LS-L46E]; Stacey Gray, *In-Store Location Tracking: A Holiday Guide*, FUTURE PRIVACY F. (Dec. 22, 2015), <https://fpf.org/2015/12/22/in-store-location-tracking-a-holiday-guid> [https://perma.cc/BC7M-YBX7].

51. Deirdre Fernandes, *More Relying on Walmart for Financial Services*, BOS. GLOBE (July 10, 2014), <https://www.bostonglobe.com/business/2014/07/09/walmart-isn-bank-but-consumers-are-choosing-its-financial-services/0oJtrqVKl8OXTuQ3SBtrSI/story.html> [https://perma.cc/5T4U-3DJ2].

52. DEZYRE, *supra* note 46.

new product recommendations.⁵³ One better-known example was when it used data analytics to determine that before hurricanes, sales in strawberry pop-tarts increase by seven times their normal rate. As a result, stores began stocking them in larger amounts before hurricanes, which led to more people purchasing them.⁵⁴ As Walmart's CEO of Global Commerce said in 2013, "We want to know what every product in the world is. We want to know who every person in the world is. And we want to have the ability to connect them together in a transaction."⁵⁵

2. *Uber*

Like Walmart, Uber has a wealth of sensitive information about its users. Users reasonably expect that Uber knows where they live and the locations they frequent; every time users interact with the app, they give the company data on at least two of their locations that day. The more often they use the service, the more Uber knows about their travel patterns. From this data, it is not hard to determine where someone works, lives, exercises, eats, and so on—any location that someone visits with regularity. Uber does not even require addresses; instead, a user may put in the name of a location (e.g., "Newark Airport" or "Starbucks"), allowing Uber to learn exactly *what* a user is visiting, rather than its location. This specificity provides Uber with information about not only users' travel patterns, but also their lifestyles—how many hours a day they spend at work, how often they sleep at home versus elsewhere, how frequently they visit a gym, what types of restaurants they go to, and much more.

Uber has a "strict policy prohibiting all employees at every level from accessing a rider or driver's data. The only exception to this policy is for a limited set of legitimate business purposes."⁵⁶ The policy does not define "legitimate business purpose" aside from examples of payment facilitation, solving problems for drivers or riders, monitoring accounts for fraudulent activity, and troubleshooting bugs. One can imagine a host of other "legitimate business purposes," including advertising or promoting the service, at the very least.

53. *Id.*

54. Hays, *supra* note 49.

55. DEZYRE, *supra* note 46; *see also* CTR. FOR MEDIA JUSTICE ET AL., *supra* note 14, at 17.

56. *Uber's Data Privacy Policy*, UBER (Nov. 18, 2014), <https://newsroom.uber.com/ubers-data-privacy-policy> [<http://archive.is/TjxGV>].

3. *Facebook & Google*

With Facebook and Google, we move into a different category, in which data sharing, collection, and usage is fundamental to the relationship between the company and the user. Not only do Facebook and Google collect data through their own websites, but they also provide data analytics tools to others. A recent study found that at least 77.4% of all websites track users' data; 60.2% of websites use Google trackers, and 27.1% use Facebook trackers.⁵⁷ This indicates that Google and Facebook also possess all of the data provided to these third-party sites as well.

People use Facebook to extend their existences onto the Internet—as “a medium for our personal lives”⁵⁸—but they have an underlying expectation that the online experience should not change that personhood. But of course it does. Seeing pictures of friends at the beach may make them more likely to want to go to the beach, seeing a friend's book recommendation may inspire them to pick it up, reading about friends' reactions to President Trump may influence their feelings about the administration (or their feelings about their friends), and so on. Especially because Facebook's newsfeed shows them what their friends are doing, rather than showing strangers, the posts they see exert a higher level of influence. Similarly, if they are using Google to find out more about the world, they do not expect that it tailors its search results to their preferences or to promote its own agenda—they assume that the search results they see are roughly the same for everyone, and differences are based on some neutral categorization. But that is not always the case.⁵⁹

Algorithms are only as good as the data put into them—if a data set is skewed, or if the code reflects its creator's implicit bias, the algorithm could be far from neutral.⁶⁰ An algorithm may treat every individual's data in the same way, but “software engineers construct the datasets mined by scoring systems; they define the parameters of data-mining analyses; they create the clusters, links, and decision trees applied; [and] they generate the predictive models

57. Many websites use multiple trackers from multiple third-party sources. *Tracking the Trackers*, GHOSTERY (Dec. 4, 2017), <https://www.ghostery.com/lp/study> [<https://perma.cc/CH9L-WM3F>]; see also Macbeth, *supra* note 6.

58. Lev Grossman, *Person of the Year 2010: Mark Zuckerberg*, TIME (Dec. 15, 2010), http://content.time.com/time/specials/packages/article/0,28804,2036683_2037183_2037185,00.html [<https://perma.cc/QES3-59GD>].

59. For a list of public updates to Google's algorithm, see *Google: Algorithm Updates*, SEARCH ENGINE LAND (last visited Nov. 20, 2017), <http://searchengineland.com/library/google/google-algorithm-updates> [<https://perma.cc/A2V8-FYUH>].

60. Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 2 (2014) (“There is nothing unbiased about scoring systems.”).

applied.”⁶¹ Even the simple choice to include or exclude a certain variable can skew an algorithm’s results.⁶² The assumption that algorithms are neutral is not just incorrect, but also potentially dangerous, as users may assume results are neutral.

It is well-documented that Facebook and Google use data to advertise, improve their newsfeed and search algorithms, and more.⁶³ The companies have the ability to know or extrapolate users’ political leanings, eating and dating habits, credit and job histories, and more. Both have a massive amount of information about each of its users, including “your age, gender, location, and everything you search for.”⁶⁴ All of this information is incredibly useful for advertising, but it can be utilized for a number of purposes, some of which would breach users’ trust. And separately, users might expect their Google search or Facebook feed to be “neutral”—that is to say, a representative sample of what other users see—when, in fact, the service provider can tailor its results to each individual viewer, based on what it knows about the user. This is not *necessarily* a breach of the fiduciary duty, but as the next Part demonstrates, it might be.

61. FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* 35 (2015).

62. See danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO. COMM. & SOC’Y 662, 667 (2012) (noting that the process of “making decisions about what attributes and variables will be counted[] and which will be ignored . . . is inherently subjective”).

63. See, e.g., Christine Erickson, *Google Privacy: 5 Things the Tech Giant Does with Your Data*, MASHABLE (Mar. 1, 2012), <http://mashable.com/2012/03/01/google-privacy-data-policy/> [<https://perma.cc/TJ2G-95UM>]; Mark Hachman, *The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers*, PCWORLD (Oct. 1, 2015, 3:00 AM), <http://www.pcmag.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html> [<https://perma.cc/DKW2-UNC2>]; Victor Luckerson, *7 Controversial Ways Facebook Has Used Your Data*, TIME (Feb. 4, 2014), <http://time.com/4695/7-controversial-ways-facebook-has-used-your-data> [<https://perma.cc/2AWF-CKP5>]; Bernard Marr, *How Facebook Is Using Big Data: The Good, the Bad, and the Ugly*, LINKEDIN (July 16, 2014), <https://www.linkedin.com/pulse/20140716060957-64875646-facebook-and-big-data-no-big-brother> [<https://perma.cc/GAA5-G286>]; Steven Rosenfeld, *4 Ways Google Is Destroying Privacy and Collecting Your Data*, SALON (Feb. 5, 2014, 12:50 PM), www.salon.com/2014/02/05/4_ways_google_is_destroying_privacy_and_collecting_your_data_partner [<https://perma.cc/4U62-LXHC>].

64. See Jeff Parsons & Sophie Curtis, *How to See Everything Google Knows About You—and Switch It OFF*, MIRROR (Aug. 21, 2017, 11:51 PM), www.mirror.co.uk/tech/how-much-google-really-know-7685863 [<https://perma.cc/YSK6-VXZF>].

III. BREACHING FIDUCIARY STATUS: FOUR MAIN PRINCIPLES

This Part attempts to elucidate the information fiduciary duty by defining four categories of behavior: manipulation, discrimination, third-party sharing, and violating a company's own privacy policy.⁶⁵ These principles were developed by the author through an examination of dozens of real and hypothetical data usage scenarios, which gave rise to common themes that emerge when people oppose specific instances of data usage. According to each principle, some practices would be permissible for information fiduciaries, while others would not. This Article posits that what separates an acceptable practice from an unacceptable one is users' expectations: if a service provider is using data in a way that reasonable users would not expect, the service provider may have violated its duty. Writ large, the reasonable person—as defined by the author and informed through public reactions to various instances of data usage over the last decade—would not expect a service provider to manipulate her with her data, discriminate against her using information it has about her, or share her data with third parties without her consent.

Additionally, the fourth principle—that service providers adhere to their own privacy policies—illuminates a crucial point regarding consent. A reasonable user would not expect a service provider to use her data in a way it has promised it would not, and so it is part of the information fiduciary duty for that reason. But it also highlights something particularly important about the information fiduciary duty: a reasonable user's expectations can—and should—shift in response to various prompts. If a company notifies users of a particular practice, that practice should come within the users' expectations. Users could then choose, of their own accord, whether or not to use the service.⁶⁶

But since it may not be possible—and certainly would not be easy—for most people to choose not to use services like Google going forward, user notification should not be a complete safe harbor. Manipulation and

65. Before diving deeper into the principles, however, it is worth noting that the fiduciary duty may not be owed to users alone; service providers may also owe a fiduciary duty to employees and independent contractors, who are also sources of data. And like users, employees and independent contractors have to simply trust that the service provider will not misuse their data. So although this Article discusses users, the protection should be extended to anyone who trusts a service provider with their personal data, such as the company's employees.

66. Although, as the author will argue, *see infra* Section III.D, privacy policies should be clearer and shorter if this is to work.

discrimination should always breach the duty, regardless of notification practices. And requiring information fiduciaries to behave in accordance with all four of these principles would also provide a level of standardization for data protection, which would “help products and services to meet consumers’ expectations” because it is easier to align expectations with reality through standardization.⁶⁷

If users reasonably trust a company with their data, the company is an information fiduciary and should act accordingly by respecting its users’ trust and expectations. If a service provider fails to do so, it will have violated its fiduciary duty and should face legal consequences. When incorporated into the duty, these four principles will adequately protect users while still allowing service providers to innovate and profit. Ideally, the hypotheticals posed after the explanation of each principle will help readers visualize the lines that must not be crossed: what would a fiduciary duty look like for service providers in practice, and how would it change the status quo? This Article focuses mainly on a set of four companies to provide consistency, but also to show how the duty varies for service providers as diverse as big box stores, ride-sharing apps, and websites that simultaneously provide social media, news, communication tools, and much more.

A. ANTI-MANIPULATION OF THE USER

A first principle of the fiduciary duty revolves around manipulation: when a company uses information about users to surreptitiously manipulate them, it may breach its fiduciary duty. And often, the user has no easy way of knowing whether and how it is happening. Cass Sunstein defines a manipulative statement or action as one that “does not sufficiently engage or appeal to people’s capacity for reflective and deliberative choice.”⁶⁸ Defined as such, manipulation can manifest in two ways: (1) a failure to respect people’s autonomy and an affront to their dignity; or (2) promotion of the welfare of the service provider over that of the user.⁶⁹ Importantly, an action is not manipulative simply because it is an attempt to alter another person’s behavior; “manipulation” is different from providing facts or attempting to persuade through reason. Instead, manipulation requires an attempt to circumvent the other person’s “capacity for reflection and deliberation.”⁷⁰ In other words,

67. See *How Standards Benefit Consumers*, ISO, http://www.iso.org/sites/ConsumersStandards/2_benefits.html (last visited Feb. 28, 2018) [<https://perma.cc/ZC8D-NB6L>].

68. Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MARKETING BEHAV. 213, 239 (2015).

69. *Id.* at 217–18.

70. *Id.* at 216.

covertness is the real concern, because users are not able to engage with the service provider or recognize its motives.

This Article draws on Sunstein's definition and analysis of manipulation to explore how service providers might manipulate users in a way that violates their fiduciary duty. As I will demonstrate, much of this would be outside what a user would reasonably expect—or detect—and thus would violate most users' trust.⁷¹

1. *A Dignity- and Autonomy-Focused Conception of Manipulation*

In one respect, manipulation is a problem because it can “violate people's autonomy (by making them instruments of another's will) and offend their dignity (by failing to treat them with respect).”⁷² In other words, manipulation is problematic when it leads someone to make a choice on terms other than their own, “depriv[ing] people of agency” or humiliating them.⁷³ Manipulation in this way breaches the trust that users place in a company when they hand over their data. Users do not expect that companies will attempt to alter their choices or decisions by using their data, particularly when the company's decision to do so is driven by its own agenda. While Google uses data to determine which websites to display in search results, the expectation is that this is an attempt to improve the service by showing the most relevant results—not an attempt to get people to do something that they would not have done otherwise. Surreptitiously manipulating the user on an important issue, such as an election, takes away users' autonomy and disrespects their conception of “self.” The fiduciary duty—designed to diminish information asymmetries—can leave no room for service providers to implement this kind of covert action.

2. *A Welfarist Conception of Manipulation*

In another respect, the problem with manipulation stems from the prioritization of one party's welfare over the other. As Sunstein explains:

71. Of course, service providers will not and should not treat all users the same; in many ways, customization is one of the advantages of the information age, for users and businesses alike. But as Jonathan Zittrain puts it, “[m]y search results and newsfeed might still end up different from yours based on our political leanings, but only because the algorithm is trying to give me what I want—the way that an investment adviser may recommend stocks to the reckless and bonds to the sedate—and never because the search engine or social network is trying to covertly pick election winners.” Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering> [https://perma.cc/AY8J-J7C2].

72. Sunstein, *supra* note 68, at 217.

73. *Id.* at 226.

“People know what is in their best interests and should have a (manipulation-free) opportunity to make that decision.”⁷⁴ Service providers engaging in this kind of manipulation may utilize data to maximize their own welfare while sacrificing the welfare of users. Users are thus deprived of the “ability to make choices on their own, simply because they are not give[n] a fair or adequate chance to weigh all variables.”⁷⁵ Service providers may not have a full and accurate picture of users’ “situation, tastes, and values,” but they “nonetheless subvert[] the process by which choosers make their own decisions about what is best for them.”⁷⁶ And if the service provider is maximizing its own self-interest, it would violate the archetypal fiduciary duty: the “special obligations of loyalty and trustworthiness toward another person. . . . The [user] puts . . . trust or confidence in the fiduciary, and the fiduciary has a duty not to betray that trust or confidence.”⁷⁷ But because users typically are unable to understand or monitor how service providers use their data, a fiduciary duty must require companies to prioritize their users’ interests over their own.⁷⁸

3. *Targeted Advertising*

The anti-manipulation principle runs up against the idea that targeted advertising—or, indeed, any advertising—is manipulative. Of course this is the case: the advertisements users are shown are meant to manipulate them into buying the featured items. Advertising is directed toward changing behavior; if someone leaves an item in a virtual shopping cart without purchasing it, an advertisement reminds her to go through with the purchase. When an advertiser shows a user a brand of makeup that is similar to the one she typically buys, it is trying to convince her to switch brands. But, crucially, users are conditioned for this; they are familiar with the concept of advertising and know that ads are meant to manipulate them. They expect service-providers will display advertisements meant to change their behavior. When they see an ad, they meet it on “equal footing”⁷⁹ and can consciously decide whether to change their behavior based on that ad. As Sunstein puts it:

In an advertising campaign, everyone knows the nature of the interaction. In some ways, manipulation is the coin of the realm. The purpose of advertisements is to sell products, and while we can find purely factual presentations, many advertisements do not appeal to

74. *Id.* at 213.

75. *Id.* at 228.

76. *Id.*

77. Balkin, *supra* note 21, at 1207.

78. *See id.* at 1227.

79. *Id.* at 1216.

reflection or deliberation at all. They try to create certain moods and associations. *To the extent that the enterprise is broadly understood, and to the extent that users understand it, the ethical objections are weakened; people can and do discount self-interested efforts at manipulation.*⁸⁰

And because of this, it is rare that the platform providing the advertising—whether print or online—is viewed as a trusted advisor in that realm. For example, there is no evidence to suggest that people trust Facebook as an advisor on the variety of products advertised through its platform, such as dating services, mortgage lenders, clothing stores, and more. Targeted advertising can be consistent with a service provider’s fiduciary duty because the manipulation is not covert. Advertising is an understood component of the relationship between a service provider and a user; it does not defeat the expectations of the end-user, even when a service provider manipulates their algorithm to better target an individual based on the data the company has about that person.

In that sense, targeted advertising is fundamentally different from a company manipulating users in a way that defeats their expectations by covertly pushing an agenda or promoting its own welfare at its users’ expense. In the first case, the agenda-pushing defeats expectations because it deprives users of agency in decision-making. In the second case, users resent the welfare-maximizing behavior as an abuse of the position of power enjoyed by the service provider. And so both forms of manipulation are unlike targeted advertising in that users neither presume that the behavior is happening nor have the information necessary to engage with the company in an informed manner. That is to say, users are familiar with the concept of advertising and usually understand that an advertisement is meant to manipulate; users are less trained to expect (and detect) manipulation from service providers and data collectors. As a result, they cannot engage with service provider manipulation in a meaningful way.

4. *Hypotheticals*⁸¹

a) Walmart Pushes an Anti-Abortion Agenda

Assume Walmart’s management and Board of Directors is staunchly anti-abortion. They make sure their website always displays sale prices for books about the mental and physical dangers of abortion, and they direct their web engineers to ensure that when someone searches online for forms of birth

80. Sunstein, *supra* note 68, at 227 (emphasis added).

81. Except where noted or cited, the hypotheticals throughout this Article are fabricated or designed to make a particular point. The author does not put forth any allegations outside of those that have been publicly reported. Any hypotheticals based on public reports have footnotes indicating the sources.

control, the results display those same books as well as advertisements featuring adorable babies. This strategy seems manipulative, but it would not violate Walmart's fiduciary duty. The key is that the company is not using each individual's data to manipulate them. Assuming these results are the same for all users, the company is free to push an agenda on customers out in the open.

But change the hypothetical so that Walmart only implements this practice for users whom it believes are white, in an effort to dissuade only white women from terminating pregnancies. This practice would violate the company's fiduciary duty. Walmart is now using a piece of data it has about the user to change its typical search results and push an agenda surreptitiously, convincing white women to have babies while letting women of other races search for birth control unimpeded. This strategy diminishes the users' autonomy in making decisions about their own health. Additionally, not only would Walmart be violating the anti-manipulation principle by using individual users' data to push an agenda, it would also violate the discrimination principle by manipulating certain groups of people based on their race and gender.⁸²

b) Uber Performs Psychological Experiments on its Drivers

In April 2017, it was revealed that Uber had performed "psychological tricks" on its employees,⁸³ to whom, as noted earlier, service providers should also owe a fiduciary duty.⁸⁴ In order to make up for its inability to require drivers to work at certain times, Uber "experimented with video game techniques, graphics and noncash rewards of little value that can prod drivers into working longer and harder—and sometimes at hours and locations that are less lucrative for them."⁸⁵ Uber used to have local managers text drivers "all day long, every day" about when the morning rush had started and where demand was highest.⁸⁶ While potentially annoying, this practice is acceptable—drivers know what is happening and why, and they can engage and respond with full knowledge.

But in addition, certain male local managers adopted female personas because most drivers are male—the theory was that men would be more likely to work harder and longer when women were the ones encouraging them to

82. The next Section describes the antidiscrimination principle in more detail.

83. Noam Scheiber, *How Uber Uses Psychological Tricks to Push Its Drivers' Buttons*, N.Y. Times (Apr. 2, 2017), <https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html> [<https://perma.cc/W8ZD-U9HA>].

84. *See supra* note 65.

85. Scheiber, *supra* note 83.

86. *Id.*

do so.⁸⁷ Uber also began using tricks well known by psychologists and video game designers: by covertly getting drivers to “internalize the company’s goals,”⁸⁸ drivers became more motivated to work longer hours. For example, research showed that drivers who completed twenty-five rides were more likely to continue driving, so Uber began sending messages at certain points, such as, “You’re almost halfway there, congratulations!”⁸⁹ When drivers attempted to log out for the day, the app would “tell them they were only a certain amount away from making a seemingly arbitrary sum for the day, or from matching their earnings from that point one week earlier.”⁹⁰ The messages were based on another psychological finding regarding people’s preoccupation with achieving goals. The company also introduced “badges” for goal achievement, another tactic cribbed from the video game industry.

Each of these tactics should be analyzed separately to determine whether a fiduciary duty would have been breached. The badges, for example, might be acceptable—a reasonable user/driver would know that these badges are meant as encouragement for driving more and can decide to use them as motivation or to ignore them. But the use of a female persona to encourage drivers to work more is less predictable and, thus, more covertly manipulative in two ways: it removes a driver’s autonomy by forcing him to make decisions based on false information, and it enhances Uber’s welfare possibly at the expense of its drivers.

To be sure, as an Uber spokesperson maintained, nothing stops drivers from ending their days; they are in literal control of that decision.⁹¹ But surreptitious tricks could be unfairly manipulative by “depriv[ing] [drivers] of agency” because they are not making decisions on their own terms.⁹² Put another way, drivers’ ultimate decisions may incorporate Uber’s influence without them realizing it, even as Uber presents itself as a company where drivers have more agency and flexibility.⁹³ Nudges may be expected in areas like targeted advertising to users, but application of these “psychological

87. *Id.*

88. *Id.* (quoting Chelsea Howe, a video game designer).

89. *Id.*

90. *Id.*

91. *Id.*

92. Sunstein, *supra* note 68, at 226.

93. *Driving Jobs vs Driving with Uber*, UBER, <https://www.uber.com/driver-jobs> [<http://archive.is/bKXIX>] (last visited Feb. 28, 2018) (“The best part about driving with Uber is that you can set your own hours. On the other hand, driving jobs, like driving a bus, can have very long hours and strict schedules. The opportunity that works best for you depends on whether you want a traditional full-time or part-time job, or want to work whenever you choose.”).

levers”⁹⁴ to the workforce could violate the trust of employees. Drivers are not aware of the manipulation, and Uber is “using what [it knows] about drivers, their control over the interface, and the terms of transaction to channel the behavior of the driver in the direction they want it to go.”⁹⁵

c) Facebook Pushes a Political Agenda, Part I

Jonathan Zittrain has posed a hypothetical about “digital gerrymandering”: on election day, Facebook “nudges” a subset of users to vote by showing them “a graphic containing a link for looking up polling places, a button to click to announce that you had voted, and the profile photos of up to six Facebook friends who had indicated they’d already done the same”—but the subset includes only those who are sympathetic to Mark Zuckerberg’s preferred electoral candidate.⁹⁶ And as Zittrain argues, “the people with the most cause for complaint are those who won’t be fed the prompt and may never know it existed.”⁹⁷

This practice violates the fiduciary duty by manipulating users to act in certain ways regarding important issues like elections. The service provider would be utilizing users’ data to pinpoint their political preferences and push them toward a particular action (or inaction). This violates users’ trust; people use Facebook on the assumption that the companies will not try to manipulate them to vote (or not vote) based on the sensitive information collected about them. Although the act of showing certain users links to find polling places is not itself manipulative, doing this on a large scale and differentiating between users based on their preferences is manipulative. Users know that Facebook’s algorithm responds to their political preferences—a user tagged by Facebook as “liberal” might see articles about Senator Elizabeth Warren and global warming rallies more than a “conservative” user. And generally, users prefer this; many users like that the algorithm makes Facebook’s newsfeeds more individually relevant. However, the expectation is that the algorithm changes *in the same way* for every user—liberals see liberal posts and conservatives see

94. Scheiber, *supra* note 83.

95. *Id.* (quoting Ryan Calo, a law professor at the University of Washington); *see also* Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623, 1630–31 (2017).

96. Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering> [<https://perma.cc/75BU-DF3N>].

97. *Id.*

conservative posts.⁹⁸ That is not the same as manipulating the algorithm so that liberal users have *more* relevant or helpful posts than conservatives do. The latter manipulation violates the trust of users, who would not reasonably expect Facebook to attempt to change their behavior in this way.

d) Google Partners with Payday Lenders for Advertising

Payday lenders in the United States often use manipulative and exploitative tactics, setting the most vulnerable consumers up to fail.⁹⁹ They advertise on the Internet, including on Google, but that does not make Google liable for their practices. But might Google's partnerships with payday lenders go further than a typical targeted advertising relationship? Companies in the financial services industry are a lucrative source of income for Google. "[T]he three most expensive categories of keyword searches as measured by cost per click are in financial services (insurance, loans and mortgages), with 45.6 percent of the top 10,000 advertising keywords falling in those categories."¹⁰⁰ Google's practice of soliciting advertisements from payday lenders is acceptable, but one reporter found that "Google is burying bad news about the industry for consumers."¹⁰¹ He discovered that Google "placed the uniformly negative news items [about payday lending] near the bottom of the results, below the fold as we used to say in the newspaper business."¹⁰² If this is in fact the case, Google is in breach of a theoretical fiduciary duty because it is manipulating users to enhance its own welfare at the users' expense. This kind of manipulation is unexpected by users; while Google's search results often change based on the user, a reasonable user would not expect that the algorithm *hides information* based on who spends the most to advertise with Google.¹⁰³

98. This may not be beneficial, writ large, but the debate on political and media silos is outside the scope of this Article.

99. Press Release, Consumer Fin. Prot. Bureau, Consumer Financial Protection Bureau Proposes Rule to End Payday Debt Traps (June 2, 2016), <https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-proposes-rule-end-payday-debt-traps> [<https://perma.cc/EK9X-KXMG>].

100. Nathan Newman, *Why Google's Spying on User Data Is Worse than the NSA's*, HUFFINGTON POST (July 1, 2013, 4:06 PM), www.huffingtonpost.com/nathan-newman/why-googles-spying-on-use_b_3530296.html [<https://perma.cc/F9WL-5E2J>].

101. *Id.*

102. *Id.*

103. And while it is true that the consumer-focused websites were shown, research has demonstrated that Google's interface gives users the "impression that the search results imply a kind of totality," but "one only sees a small part of what one could see if one also integrates other research tools." See H. MAURER ET AL., REPORT ON DANGERS AND OPPORTUNITIES POSED BY LARGE SEARCH ENGINES, PARTICULARLY GOOGLE 16 (2007),

Some have accused Google of maintaining “ads from fraudulent mortgage ‘loan modification’ firms preying on desperate homeowners even after the company was alerted to the problem.”¹⁰⁴ This is likely not a form of manipulation unless Google’s Terms of Service promise that it will not show advertisements from these kinds of companies. Google should not be held liable for displaying advertisements from companies that implement illegal practices. Not only would it be overly burdensome for Google to have to look into its advertisers’ practices—in a wide variety of industries, all with different regulations—but it should also be unnecessary for a fiduciary. Because this falls into the category of targeted advertising, we should trust users to know an advertisement when they see it. Google should not be on the hook for every bad actor who buys advertisement space.

B. ANTIDISCRIMINATION

The second principle that information fiduciaries must follow is antidiscrimination, or refraining from discriminating between or against users based on characteristics like race or gender. The set of data points available to companies often includes these qualities and many others. There are three main methods by which a company might discriminate based on these characteristics: (1) access to services, (2) prices, and (3) digital redlining. As a fiduciary, a firm must not offer different services or prices to individuals based on their membership (or non-membership) in a protected class. Users likely do not expect that when they hand over their data online, they are making it easier for companies to discriminate against them or others, or that the company will in fact do so. If users do not expect this type of practice, they cannot reasonably guard against it by choosing service providers more carefully or choosing not to provide certain data about themselves. Companies can triangulate to figure out a user’s characteristics (for example, extrapolating someone’s age and gender from the websites they visit and products they buy), and users are unlikely to expect or believe that they should hide this information about themselves.

Furthermore, users often have no choice but to provide their data—not just because it is difficult to operate in the modern world without Google or Facebook, but also because many other important services require it. For example, to cash a payroll check at Walmart—a service relied on by many

http://www.iicm.edu:8080/Ressourcen/Papers/dangers_google.pdf [https://perma.cc/ZF4G-GZUR].

104. Newman, *supra* note 100.

people with low income¹⁰⁵—you must give them your Social Security number, which opens the door to a host of data about the customer.¹⁰⁶ Because service providers have an immense upper hand in gathering and using this information, they should be required to treat it with the utmost care.

When considering “discrimination,” it is important to determine what qualities service providers could use to discriminate. Many are those that define membership in a protected class: race, color, religion, national origin, age, sex (gender), sexual orientation, and physical or mental disability.¹⁰⁷ However, Big Data makes it unwise to focus only on traditional targets of discrimination, such as racial minorities. As more data emerges, it may become the case that the people against whom firms discriminate do not correspond with the traditional categories listed above. When service providers collect data that lets them identify and categorize users by hundreds of categories, it becomes easier to isolate and discriminate against a new group: those who are less “valuable.” For example, it may be the case that white men of a certain socioeconomic status and in a certain geographic area are less valuable to service providers because fewer advertisers are interested in reaching them. And, as with all discrimination, offering certain services or products only to “valuable” groups further entrenches divisions or silos that already exist. The antidiscrimination principle, then, involves a moving target that will need to be reassessed periodically to identify who may be harmed or left behind by algorithmic decision-making.

1. *Access to Services*

One way in which companies could discriminate against users is by offering different services to different people. For example, if a Facebook algorithm determines that the data of young people is more valuable than the data of older people, it could continue offering Facebook for free to young people, while providing older people with only a pared-down, barer platform. Or, the company could provide more tools or apps for younger people than older people. A company might not want to waste expensive server space on users who generate less advertising revenue. More subtly, this type of discrimination could be mixed in with a “freemium” model of services, which

105. About a fifth of Walmart customers are unbanked, and Walmart processes 1.2–1.4 million money orders, wire transfers, and cashed checks per week. JEAN ANN FOX & PATRICK WOODALL, CONSUMER FED’N AM., CASHED OUT: CONSUMERS PAY STEEP PREMIUM TO “BANK” AT CHECK CASHING OUTLETS 14 (2006), http://www.georgiawatch.org/documents/CFA2006CheckCashingStudy_000.pdf [<https://perma.cc/JB9M-PDZT>].

106. Hays, *supra* note 49.

107. *EEO Terminology*, NAT’L ARCHIVES (Aug. 16, 2015), <https://www.archives.gov/eo/terminology.html#d> [<https://perma.cc/ZT3L-4NJE>].

typically offers a basic service for free and then charges a price for the premium service. For example, Spotify offers its basic platform for free, but charges a monthly fee for users to avoid commercials and access the platform on more than one device.¹⁰⁸ Spotify could easily alter this model to create different options for different users based on certain characteristics, such as age, gender, profession, geolocation, amount of money spent with other service providers, and much more.

Service discrimination likely defies most users' expectations of service providers when they engage in a typical online transaction. When people use Facebook, they do not expect that they are seeing more or fewer features (for example, a newsfeed, group invitations, or applications like Candy Crush) based on their personal characteristics. Imagine if Facebook only offered newsfeeds or posting capabilities to people who make a certain amount of money or work in certain fields—this kind of discrimination would undermine the expectations of all users. When those users provided Facebook with their information, it likely never occurred to them that the information could then be used to limit or grant access to specific features. A service provider would be breaching its fiduciary duty by using the data users provided to offer them an incomplete suite of services.

To be fair, tailored services are often seen as a feature of Big Data, rather than a bug. The fact that a service provider can change services based on a user's interests can improve the service itself: for example, if Facebook knows that a user is a runner, and thus proactively offers a free running map application to that user, it may be mutually beneficial for both user and service provider. And someone who prefers Game of Thrones fan fiction to running may prefer that Facebook populates her newsfeed with Game of Thrones fan pages instead of a running map application. But this is not discrimination as long as the services are *available* to both people. A service provider can affirmatively offer services to users who might be interested, but to be a fiduciary, it should not *prevent* any user from accessing a service that is available to some. The runner may have to actively search for the Game of Thrones pages if she wants to view them, but as long as they are available to her, the practice is consistent with the fiduciary duty.

108. Pascal-Emmanuel Gobry, *How Spotify's Business Works*, BUS. INSIDER (Oct. 12, 2011, 12:53 PM), <http://www.businessinsider.com/how-spotifys-business-works-2011-10> [<http://archive.is/yYtct>].

2. Price Discrimination

Data collection also makes price discrimination easy. A company could identify who might be more likely to pay higher prices or at what times they are more likely to do so and then shift pricing based on that information. For example, Walmart could increase the price for pop-tarts before a hurricane, as noted above,¹⁰⁹ or Uber could charge women more at night based on data that women are more likely to take cars than they are to walk after dark. Both of these practices might be based on data and algorithmic results. The first example would be permitted because it does not target a specific group of people. The change in pop-tart pricing would be based on publicly available data, such as timing and weather patterns. But the second example should be prohibited for fiduciaries, since it disadvantages a group based on data about users' gender obtained for another purpose.

Of course, price discrimination occurs all the time, such as with senior citizen discounts or variance in gas prices.¹¹⁰ But these are instances of price discrimination about which users are aware. Senior citizen discounts are clearly posted, and a reasonable driver knows that gas prices vary by location, mirroring the other cost-of-living adjustments she sees in different parts of the country.¹¹¹ More often than not, comfort with certain types of price discrimination coincides with user expectations having been shifted. A user of an online service provider, however, cannot tell if “companies are offering discounts to higher-status customers in the first place.”¹¹² Few would expect that the prices for items like kitchen tools or clothing on a standard website change based on who is viewing the item. And it would be quite difficult to identify when a company adds a dollar to certain products if it believes the person viewing them online is black, for example, especially because false negatives and positives would occur and confuse even rigorous analyses.¹¹³

109. As discussed earlier, Walmart's data shows that strawberry pop-tart sales increase seven-fold before hurricanes. Hays, *supra* note 49.

110. See Jennifer Valentino-DeVries, Jeremy Singer-Vine & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), <http://www.wsj.com/news/articles/SB1000142412788732377204578189391813881534> [<https://perma.cc/LC2P-3WWW>].

111. See *Gasoline and Diesel Fuel Update*, U.S. ENERGY INFO. ADMIN. (Nov. 23, 2017), https://www.eia.gov/petroleum/gasdiesel/gas_geographies.php#pricesbyregion [<https://perma.cc/Y96J-HQGJ>].

112. Jeffrey Rosen, *Who Do Online Advertisers Think You Are?*, N.Y. TIMES (Nov. 30, 2012), <http://www.nytimes.com/2012/12/02/magazine/who-do-online-advertisers-think-you-are.html> [<https://perma.cc/KZM8-CGFG>].

113. This is not a worst-case scenario supposition either. As a 2013 article notes, people of color and low-income communities face particular risks. The “poverty exception” to privacy rights has been explored previously, see Christopher Slobogin, *The Poverty Exception to the Fourth*

This type of conduct undermines the economic and psychological interests of users by utilizing their data to discriminate more efficiently.

There is no way for a single user to know whether they are seeing a higher price online than someone of a different race sees and no cost-effective way for them to figure it out. And fiduciaries should not engage in practices that force consumers to band together to police them. Because this type of discrimination is both economically harmful and opaque, it is unreasonable to expect users to know whether a company is using information it has about them to decide what to charge them for goods and services. Users cannot engage with the service provider on an equal footing in this context, and the company is abusing its power and breaching users' trust.

3. *Digital Redlining*

While it is not clear that many companies are currently offering different services or prices based on membership in a protected class, service providers can discriminate by zip code, which can often be a proxy for membership in a protected class. Though now illegal, practices such as redlining¹¹⁴ have enabled this type of discrimination in the past. Now, this type of discrimination is easier with Big Data. Internet Protocol (IP) addresses can be linked to zip codes—this allows most firms to know where their users are when they access a website.¹¹⁵ There is no general statute that proscribes online service companies from shifting their service offerings or prices by zip code. And even if they are using zip codes in this way, it may be defensible in court as a business necessity—assuming a user could even figure out that the practice is occurring and get into court.

Amendment, 55 FLA. L. REV. 391, 412 (2003), and the risks of bias or discrimination based on the inappropriate generation of personal data—what have been called “predictive privacy harms”—are well-documented, see Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 95 (2014); see also FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (2015); Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE 25 (2013); Kevin Tobia, Note, *Disparate Statistics*, 126 YALE L.J. 2382 (2017).

114. Redlining is “the illegal practice of refusing to offer credit or insurance in a particular community on a discriminatory basis (as because of the race or ethnicity of its residents).” *Redlining*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/legal/redlining> [<http://perma.cc/6BFU-6469>].

115. See, e.g., *Geolocate IP Address Location Using IP2Location*, IP2LOCATION, <https://www.ip2location.com> [<https://perma.cc/FU34-K2DN>] (last visited Feb. 28, 2018); *IP Address Lookup*, WHATISMYIP.COM, <https://www.whatismyip.com/ip-address-lookup> [<https://perma.cc/DP4X-36A2>] (last visited Feb. 28, 2018).

Of course, markets and demand differ across the United States; it is understandable that Uber might charge more in an established market like New York than in a market in which it is newer and less popular. It is not only understandable, but perhaps preferable, that when one searches for restaurants on Google, the search results show places in the user's area.¹¹⁶ Information fiduciaries exist in a vast number of industries, some of which appropriately discriminate by zip code. For example, nanny services offered via Care.com are more expensive in San Francisco, California than they are in areas with lower costs of living, like Fargo, North Dakota.¹¹⁷ The ability to adjust pricing according to cost of living is not in itself problematic.

But price differentials should be tied to market demand rather than racial or other biases. To use mortgage lending as an analogy: houses are priced based on their location, but they cannot be priced differently based on the buyer's identity. In the former case, the price is derived from market demand; in the second, it could be derived from discrimination. A similar principle should apply across the board—demand differs by market, and prices can adjust accordingly. But prices should not differ based on buyers' identities. If a geolocation-based practice were challenged in court, a “substance-over-form”-like doctrine¹¹⁸ should be applied; a court could consider whether, agnostic of any protected class disparities, market economics demanded differential pricing or services in specific areas.

In certain cases, geographic discrimination might be consistent with a fiduciary duty. Discover has “show[n] a prominent offer for [its] new ‘it’ card” to users in particular cities and Rosetta Stone has offered discounts and

116. However, this justification can become a slippery slope: proponents of redlining in the mortgage space also argued that it simply made sense from a business perspective to refuse to lend in certain areas. But this practice “perpetuate[s] historical conditions . . . [and] helps to promote a racially separate and unequal distribution of political influence and economic resources.” Richard Thompson Ford, *The Boundaries of Race: Political Geography in Legal Analysis*, 107 HARV. L. REV. 1841, 1844 (1994).

117. *Compare San Francisco Nannies*, CARE.COM, <https://www.care.com/nannies/san-francisco-ca> [<https://perma.cc/77UC-3GYC>] (last visited Feb. 28, 2018) (listing the average price for a nanny in San Francisco as \$17.25 per hour), *with Fargo Nannies*, CARE.COM, <https://www.care.com/nannies/fargo-nd> [<https://perma.cc/W923-R6DV>] (last visited Feb. 28, 2018) (listing the average price for a nanny in Fargo as \$10.75 per hour).

118. In tax, the substance-over-form doctrine allows a court to “recharacterize a transaction in accordance with its substance, if ‘the substance of the transaction is demonstrably contrary to the form.’” DEP’T OF TREASURY, THE PROBLEM OF CORPORATE TAX SHELTERS DISCUSSION, ANALYSIS AND LEGISLATIVE PROPOSALS vii–viii, 47 (1999). In other words, if the court can tell a litigant was trying to achieve one outcome while making it look like something else, the court can respond to the reality of the transaction, not its appearance. *See id.*

“bundles” in particular locations.¹¹⁹ These are plausible cases in which a non-discriminatory market analysis might explain the company’s decision. On the other hand, ProPublica discovered that “Asians were nearly twice as likely to get [a] higher price from The Princeton Review than non-Asians” for an SAT course.¹²⁰ Prices were charged based on zip code, not based on race, but in at least one example, a Queens zip code with 70.5% Asian residents but a below-median average income was charged the highest price possible for the course.¹²¹ Absent another justification for the pricing disparity, it seems that Princeton Review may have specifically targeted Asians, as the disparity cannot be explained only by the zip code’s average income level.¹²² Even if one argues that Asians *are* more likely to pay higher prices for SAT courses, and so Princeton Review was simply responding to market demand, service providers should not be permitted to use the data they have on users’ race to respond to market demand. Users who provided that information when signing up for a course online would never have expected that data to be used to then charge them a higher price.

4. *Hypotheticals*

a) Advertising Products Based on Broad Demographic Preferences

Many retailers’ websites show products that a user might like based on other items the user has purchased or browsed. Assume a person buys L’Oréal shampoo from Walmart every few months, and assume Walmart’s data demonstrates that when L’Oréal’s price goes up, women typically switch to Dove shampoo, while men switch to Suave. Walmart might share this finding with Dove and Suave, who could then pay Walmart to show advertisements for Dove to women and Suave to men who search for L’Oréal online. This practice would be entirely consistent with the fiduciary duty. Even though the

119. Valentino-DeVries et al., *supra* note 110.

120. Julia Angwin, Terry Parris Jr. & Surya Mattu, *When Algorithms Decide What You Pay*, PROPUBLICA (Oct. 5, 2016), <https://www.propublica.org/article/breaking-the-black-box-when-algorithms-decide-what-you-pay> [<https://perma.cc/L3UY-7Z83>].

121. Julia Angwin & Jeff Larson, *The Tiger Mom Tax: Asians Are Nearly Twice as Likely To Get a Higher Price from Princeton Review*, PROPUBLICA (Sept. 1, 2015, 10:00 AM), <https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review> [<https://perma.cc/FT32-MGGT>].

122. Certainly, there could be a third variable that explains the disparity, or the Rosetta Stone and Discover examples could be driven by a discriminatory motive. But absent additional information, the contrast between the two demonstrates that location-based “deals” can work if they do not discriminate based on sensitive user data.

advertising does “discriminate” based on gender, the discrimination is part of a targeted advertising campaign and is thus within users’ expectations.¹²³

However, assume Walmart instead determined that black people prefer L’Oréal and white people prefer Suave. Then, it chose to limit choices in a store in a predominantly black neighborhood and hike up the price for L’Oréal, and do the same for Suave in a predominantly white neighborhood. This would be an unacceptable use of race data. No longer is Walmart using data to perform targeted advertising with which users can engage on equal footing. Instead, in this second hypothetical, Walmart has skipped the advertising altogether and would be using data to charge higher prices for a product it knows that a certain demographic group wants.

b) Walmart Changes Shipping Prices Based on Zip Code

Walmart—and most stores—charge a shipping fee for online orders. Walmart may know that in high-income suburban neighborhoods where people are more likely to have cars, the user may just drive to the nearest store if the shipping fee is too high. The brick-and-mortar store they choose may or may not be a Walmart. In low-income neighborhoods where people may not have cars or easily accessible brick-and-mortar stores, users may be more likely to purchase certain items online, subjecting them to a shipping fee. Walmart could charge more for shipping in neighborhoods without easily accessible brick-and-mortar stores. This seems to violate the discrimination principle, though we may have to dig deeper.

It might be the case that it actually is more expensive to ship to these areas, though this is a more plausible argument for a zip code in a rural area than for a low-income zip code in a big city. And if Walmart could prove that the price hike was only given to those in neighborhoods where shipping is actually more expensive, it might survive a legal challenge. However, if Walmart were uniformly charging more in neighborhoods where no brick-and-mortar stores are nearby, regardless of the actual cost of shipping, it would be violating its fiduciary duty because users are not given a choice or enough information to make an informed decision. In the first shampoo example, users understand that they are being advertised to; here, there is no equivalent framework with which users are familiar.

123. On the other hand, the example in Section III.B.4.e below is not a targeted advertisement—it simply uses gender and other data to charge women more. No advertisement or notice is given.

c) Amazon Prime's Free Same-Day Delivery Service

Contrast Amazon Prime's Free Same-Day Delivery service, which, as of April 2016, was offered in twenty-seven metropolitan areas.¹²⁴ In many of those cities, "predominantly black ZIP codes" are excluded from the service.¹²⁵ In at least four cities, "black citizens are about half as likely to live in neighborhoods with access to Amazon same-day delivery as white residents."¹²⁶ Amazon maintains that zip codes are included or excluded based on the number of Prime members in those zip codes, and that it would be too expensive to include zip codes with few customers. It is at least plausible that this is true. But in Washington, D.C., the excluded zip codes east of the Anacostia River are quite close to downtown—closer, in fact, than some other D.C. metro areas that do receive same-day delivery service.¹²⁷ According to Google Maps, a zip code in Manassas, VA (20110) is 31 miles from the White House, the center of downtown D.C., and a zip code in Anacostia (20032) is 8.5 miles from the White House. But only the Manassas zip code receives the free same-day delivery service. If this were challenged in court, the court would need to delve deeper into the economics to decide whether this model violates the company's fiduciary duty. If exclusion of the black zip codes is, in fact, based on the fact that delivery to Manassas is significantly less costly than delivery to Anacostia, it might be acceptable. But if the economics do not quite make sense, the practice might violate the fiduciary duty.

d) Uber's Surge Pricing

Uber uses "surge pricing": when Uber is in high demand in a certain area, such as after a sporting event or during a rainstorm, prices are raised to ensure that those who are most willing to pay receive cars. This is basic market economics, and since everyone in the same area is offered the surge price at the same time, it is consistent with a fiduciary duty. But one can imagine a surge pricing-like technique that is similarly based on demand, but applied in a more discriminatory way. Imagine that Uber started charging women higher

124. Amit Chowdhry, *Amazon Adds 11 More Cities to Same-Day Delivery Service*, FORBES (Apr. 8, 2016, 3:19 PM), <https://www.forbes.com/sites/amitchowdhry/2016/04/08/amazon-adds-11-more-cities-to-same-day-delivery-service/> [https://perma.cc/6Q5B-DAHF].

125. David Ingold & Spencer Soper, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, BLOOMBERG (Apr. 21, 2016), <https://www.bloomberg.com/graphics/2016-amazon-same-day> [https://perma.cc/8SJ2-EP3S].

126. *Id.*

127. Rachel Sadon, *Amazon Adds Free Same-Day Prime Delivery to D.C.—Well, Certain Parts of D.C.*, DCIST (May 29, 2015, 4:14 PM), http://dcist.com/2015/05/amazon_adds_free_same-day_delivery.php [https://perma.cc/WA9A-Z2Z7].

rates in cities at night because Uber's data demonstrates that women are more likely to pay a higher price for the service because they feel less safe walking home than a man would feel. Uber could implement this system by identifying every user's gender and shifting prices based on that information, the time of day, and the user's location. This is an example of data confirming, and possibly entrenching, stereotypes that already exist—the fact that data may seem to support a stereotype about a particular group of people should not be enough to permit a firm to take advantage of that stereotype.

This practice would violate the discrimination principle. Uber is choosing a class of people based on data it has about their gender—and a particular vulnerability due to that gender—and charging them more. When users entrust Uber with their data, they should reasonably expect surge pricing, because the app makes it clear when it is happening through an alert. However, users have no reason to expect or predict that Uber will also exact a “vulnerability fee” because it knows when a user is a woman. By doing so, Uber would violate users' trust.

e) Facebook Buys a Mortgage Lender

Facebook could purchase a mortgage lender and make it a subsidiary of its holding company. It could then potentially allow loan officers at the subsidiary to access users' Facebook data or social networks when deciding whether or not to extend credit to those users.¹²⁸ Certainly, discrimination based on race, gender, national origin, or something similar would be illegal under existing law. But assume the loan officers do not incorporate any of that data into their decisions. Instead, they focus on other things about you—your spelling and grammar, your educational background, your friends, your social activities, and more. A lender cannot refuse to extend credit based on an applicant's race, but can she refuse to lend (or raise the price) based on the race or education level of a prospective borrower's friends?¹²⁹ What about the fact a user frequently misspells words in posts, or that they frequently link to “fake news” sites? While this is not digital redlining because it is not based on zip code, it feels similarly underhanded. People expect lending decisions to be made on directly

128. In fact, Facebook has patented technology that would purportedly allow “lenders to use a borrower's social network to determine whether he or she is a good credit risk.” See Ananya Bhattacharya, *Facebook Patent: Your Friends Could Help You Get a Loan—or Not*, CNN (Aug. 4, 2015, 6:58 PM), <http://money.cnn.com/2015/08/04/technology/facebook-loan-patent> [<https://perma.cc/F3CR-K7XW>].

129. See Robinson Meyer, *Could a Bank Deny Your Loan Based on Your Facebook Friends?*, ATLANTIC (Sept. 25, 2015), <https://www.theatlantic.com/technology/archive/2015/09/facebook-new-patent-and-digital-redlining/407287> [<https://perma.cc/NP2A-XKZM>] (“Since one's friends so closely mirror one's race and class—according to one study, nine out of 10 of the average white American's friends are also white—the practice would effectively restore loan discrimination.”).

relevant information—credit histories, salaries, and the like. On the other hand, lending decisions made based on a user’s Facebook posts or friend network are not only unexpected, but could also unfairly discriminate against certain populations. In the worst-case scenario, it could be a way for a lender to get around antidiscrimination law by using proxies for race. If it could be proven that this practice had disparate impact on minority borrowers, it would likely be discriminatory and in contravention of Facebook’s fiduciary duty.

C. LIMITED SHARING WITH THIRD PARTIES¹³⁰

Discrimination and manipulation both focus on what a company might do internally that would disregard a user’s reasonable expectations or violate the user’s trust. A third concern is more external-facing: to whom can a fiduciary disclose a user’s data?¹³¹ Service providers often have privacy policies in which they identify third parties with whom they share user information. But in some cases, sharing personal information may be a violation of trust: users may have shared data based on their relationship with and confidence in Company A, which does not extend to Company B. The users might not have disclosed that information in the first place if they had known Company B would have access to it; in this way, sharing takes away users’ agency and choice over who accesses their data. But beyond the user’s distrust of Company B, Company A’s act of sharing her personal data changes the relationship between the user and the

130. This Article explicitly focuses on consumer privacy in the private marketplace. Much has been written—and remains to be written—on the government’s usage of data and on private firms sharing data with the government. *Carpenter v. United States*, for example, a case heard by the Supreme Court in October Term 2017, will address the warrantless search of cellphone records that indicate the user’s location and movements over several months. *Carpenter v. United States*, 137 S. Ct. 2211 (2017) (granting certiorari). But this Article leaves government data collection to be dealt with separately. In order to focus on the heart of the information fiduciary duty, the author has chosen to avoid complicating the analysis by introducing a host of other laws and standards which are necessarily at play in government data collection. That said, the government should also have to abide by certain standards in data collection and usage.

131. This Article focuses on voluntary disclosure or sale of data. Hacking is also a concern. However, for the purpose of this Article, it suffices to say that a company may also breach its fiduciary duty by not securing data properly, or not notifying users promptly when a hack has occurred. *See, e.g.*, Greg Bensinger & Robert McMillan, *Uber Reveals Data Breach and Cover-Up, Leading to Two Firings*, WALL ST. J. (Nov. 21, 2017, 11:38 PM), <https://www.wsj.com/articles/uber-reveals-data-breach-and-cover-up-leading-to-two-firings-1511305453> [<https://perma.cc/24CA-W94W>]. Because hacking is generally not purposeful on the part of the hacked firm, it does not fall into the category of things the company could do affirmatively to breach its duty.

company; once Company A shares a user's personal data, the user's trust in the company has been undermined.¹³²

The identities of third parties with whom service providers may share information varies widely from provider to provider. From a user's point of view, some of these likely seem reasonable—for example, that Facebook shares the information a user posts with their selected audience (most likely their friend network), and that Uber shares a user's information with drivers. However, some of this sharing is less predictable, such as Uber's sharing of information with “vendors, consultants, marketing partners, research firms, and *other service providers or business partners.*”¹³³ This last category is disturbingly vague, especially because it is clear that this portion of the policy refers to personally identifiable information. The list *later* references aggregated data (which Uber may share with any third parties, according to its policy), indicating that the earlier provision applies to non-aggregated, or personally identifiable information.¹³⁴

1. *Identities and Obligations of Third Parties*

In considering a fiduciary duty for service providers, it is important to decide with which third parties data can be shared consistent with users' expectations. For the purposes of this Article, third parties are defined as companies other than the end-user and the service provider with whom the end-user directly interacts. It is difficult to identify every type of third party and categorize whether a service provider who wants to maintain fiduciary status can give them data. Circumstances change, and users' expectations of Uber, for example, may be different than their expectations of Facebook or Walmart. However, there are a few rules of thumb that may help define “third parties.” In all cases, a company that receives user data from a service provider must immediately become an information fiduciary to the individuals included in the dataset, and thus comply with all responsibilities of the original fiduciary. In no situation should a service provider share data with a company that does

132. Cf. Morgan Hochheiser, Comment, *The Truth Behind Data Collection and Analysis*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 32, 52 (2015) (“Selling data exploits a consumer and therefore is against public policy. The public needs to trust businesses and the government, but if businesses sell private information and the government allows it, the public has no one to trust with their PII.”).

133. *Privacy Policy*, UBER (Sept. 21, 2017), <https://privacy.uber.com/policy> [<https://perma.cc/4K8M-7TWW>] (emphasis added).

134. *Uber Privacy Statement 2015*, UBER (July 15, 2015), <https://d3i4yxtzktqr9n.cloudfront.net/privacy-policy/static/past-policies/privacy-policy-2015-en-1244ec7107.pdf> [<https://perma.cc/4KDN-H6TJ>] (“We may share your information . . . [i]n an aggregated and/or anonymized form which cannot reasonably be used to identify you.”).

not uphold an information fiduciary duty; doing so knowingly would be a violation of the company's own duty as well.

Subsidiaries of the same holding company and “partners” are often recipients of user data. Sharing of user information with these kinds of recipients should be allowed when it enhances the service being provided—not merely when it “helps business” in some vague way. For example, Waze Mobile,¹³⁵ whose parent company is Alphabet, Inc., should be able to share data with Google Maps, since the integration of traffic data is part of the service that users appreciate and on which they rely. However, many companies are subsidiaries of holding companies which parent several seemingly unrelated businesses. For example, Alphabet also owns Zagat,¹³⁶ a company that rates restaurants, and Nest,¹³⁷ a company that makes smart-home thermostats.¹³⁸ Users may not expect that by using Zagat's phone app, they are providing data that may be shared with Nest and Waze. Whether this sharing violates the fiduciary duty should be determined case-by-case based on whether a reasonable user would have expected it.

Advertisers are often third parties as well. While targeted advertising is a necessary component of many business models, it does not require that individual user data be shared with advertisers. Instead, advertisers should identify groups they want to target (for example, women between the ages of twenty to thirty who have expressed an interest in a particular television show, activity, food, and so on), and the service provider should identify the actual targets. While targeted advertising as a phenomenon is often in users' interests since it keeps the cost of services down by generating higher advertising revenues, there is no need for individuals' information to be shared with advertisers to make this business model work. As such, it would be inconsistent with a fiduciary duty to share user information with third parties.

An additional third party is trackers—companies who provide analytical tools to websites that want to collect or utilize user data. Fifteen percent of

135. Darrell Etherington, *Google's Waze Acquisition Bears First Fruit As Mobile Google Maps App Gets Real-Time Incident Reports*, TECHCRUNCH (Aug. 20, 2013), <https://techcrunch.com/2013/08/20/googles-waze-acquisition-bears-first-fruit-as-mobile-google-maps-app-gets-real-time-incident-reports/> [https://perma.cc/F8V4-EGTT].

136. ZAGAT, <https://www.zagat.com> [https://perma.cc/RG73-KYYY] (last visited Feb. 28, 2018).

137. NEST, <https://nest.com> [https://perma.cc/BAL9-ZATX] (last visited Feb. 28, 2018).

138. Mike Murphy & Akshat Rathi, *All of Google's—er, Alphabet's—Companies and Products from A to Z*, QUARTZ (Aug. 10, 2015), <https://qz.com/476460/here-are-all-the-alphabet-formerly-google-companies-and-products-from-a-to-z> [https://perma.cc/4STQ-H46L].

global websites share private data to ten or more tracker operators.¹³⁹ Facebook and Google are the biggest providers of tracking tools, though a number of companies offer them.¹⁴⁰ These companies are essential to websites that want to benefit from data collection. But as third-party recipients of data, they should bear the same fiduciary responsibilities as the primary website with which the user interacts. For example, the Mayo Clinic website uses a number of trackers; it also allows users to learn about HIV tests and make appointments.¹⁴¹ The Mayo Clinic should have a fiduciary obligation with regard to that data, and so should the third-party tracker that the Clinic uses.

Another potential third party with which data can be shared is an aggregator, such as Acxiom, a company that, as of 2013, owned about 1,500 data points¹⁴²—including “household income, ZIP code, race, ethnicity, social network or interests like ‘smoking/tobacco’ or ‘gaming-casino’ ”¹⁴³—on 700 million individuals.¹⁴⁴ Aggregators collect data from thousands of sources and aggregate fuller profiles on individual users, presenting a host of problems for fiduciaries. Users conceive of their relationships with various companies as separate from each other; when a user tells Facebook that she enjoys cooking, she does not expect Blue Apron, Stop & Shop, or Amazon/Whole Foods to be able to purchase a list with her name and email address. But an aggregator can match her email address with Google searches to identify how often she searches for recipes or her Facebook profile to show that she often posts photos of food. The aggregator can then sell that much more valuable profile to any number of companies.

But Acxiom and companies like it cannot be information fiduciaries to anyone—the fiduciary relationship requires that users know a company is collecting their data and that users have placed some sort of trust in that company. Users do not willingly give their data to companies like Acxiom; “consumers are often unaware of the existence of data brokers as well as the purposes for which they collect and use consumers’ data.”¹⁴⁵ So when

139. See GHOSTERY, *supra* note 57.

140. See Macbeth, *supra* note 6, at 5-6.

141. See GHOSTERY, *supra* note 57.

142. Katy Bachman, *Confessions of a Data Broker*, ADWEEK (Mar. 25, 2014), <http://www.adweek.com/digital/confessions-data-broker-156437> [<https://perma.cc/SD74-G3MG>].

143. Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, N.Y. Times (Feb. 27, 2015), <https://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html> [<https://perma.cc/6XHM-MU26>].

144. Bachman, *supra* note 142.

145. Press Release, Fed. Trade Comm’n, FTC to Study Data Broker Industry’s Collection and Use of Consumer Data (Dec. 18, 2012), <https://www.ftc.gov/news-events/press->

aggregators create this fuller profile, often facilitating discrimination and manipulation, users are unaware of its existence. For this reason, no fiduciary should be able to share data with a company whose business model is built on collecting data from many sources and selling fuller profiles, and no fiduciary should be able to purchase and/or utilize data collected by one of these companies.

Data can be shared in an identifiable format or in an aggregated format. The discussion above covers the sharing of identifiable information. Sharing aggregated data with third parties is consistent with an information fiduciary duty if no individual is personally identifiable and there are no unique identifiers for any one person.¹⁴⁶ Aggregated datasets may help companies provide better service without posing much risk of harm to individuals. If a company aggregates data to identify products that are preferred by a certain demographic group or to determine usage behavior by certain groups or at certain times, that information could help their business without breaching any individual's trust. But if the aggregated data is used to discriminate against or manipulate users—thus violating the principles outlined above—it would still violate the fiduciary duty.

One could argue that even aggregated data-sharing can be harmful. For example, what if a company discovers and publicizes that a certain age and racial group is particularly susceptible to cigarette advertisements, encouraging tobacco companies to target those people? Many people might see this as a negative outcome, but it must be separated from the principle of data privacy. No individual's privacy has been breached, and the company has not breached its fiduciary duty. An argument that the company did not use those individuals' data in their best interest would also require companies to make judgments about which products are "good" and which are "bad." Companies should be able to be neutral in their data sharing; we should allow Facebook to aggregate and sell a report about exercise trends and smoking trends because the law should not be making those kinds of judgments through privacy policy.

releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data [https://perma.cc/N2US-T7DG].

146. For example, it should not be possible for two companies to create a unique identifier system such that their datasets are easily combined and individuals become identifiable.

2. *Hypotheticals*

a) Uber Broadcasts the Locations of Well-Known People at a Launch Party

As mentioned in Part I, Uber projected the real-time location of Peter Sims, an angel investor, on a wall during their Chicago launch party.¹⁴⁷ The third party here is not someone who would buy the data to enhance their own business; here, Uber shared an individual's data with a third party (the party attendees) to market its product. This violates the company's fiduciary duty by breaching the user's trust; the sharing did not enhance the service for Sims—in fact, as he explained, it weakened it—and it was certainly unexpected. After Sims learned from a friend that Uber had displayed his location and the location of other “NYC certain ‘known people,’ . . . I expressed my outrage to her that the company would use my information and identity to promote its services without my permission. She told me to calm down, and that it was all a ‘cool’ event and as if I should be honored to have been one of the chosen. What nonsense.”¹⁴⁸

But if Uber had just displayed the location of one hundred anonymous celebrities, there might be no way to determine which celebrities were being tracked. This could be consistent with the fiduciary duty if no individual's data were traceable back to them. Merely displaying the data in real-time on a wall does not leave much room for disaggregation, and because no rider is identifiable, Uber could be within its rights to do this.

b) Facebook Tells Someone's Friends About Their Purchases

Facebook and other platforms are integrated with many other sites. When users buy something from a clothing store's website, they can often sign into that website using their Facebook logins, which then grants Facebook varied levels of access to their interactions with the clothing website. Facebook may know what items users purchased, and could then present their friends with advertisements (presumably in concert with the store) that display the items and mention that a friend purchased it. This could be potentially embarrassing; what if it is a personal item about which you would not have told your friends, such as a self-help book, a particular medication, or a financial product? But that does not mean it is inconsistent with the fiduciary duty. First of all, when a user provides her Facebook username and password to log into another website, there is a pop-up that explains what data will be available to whom.

147. Sims, *supra* note 1.

148. *Id.*

The notification, in its current form, is typically short and clear¹⁴⁹ and may be enough to shift a reasonable user's expectations of the companies involved.¹⁵⁰ The resulting third-party sharing should, then, be within the user's expectations; trusting Facebook to *not* use or share this data once a user has been warned would be unreasonable.¹⁵¹

But shift the hypothetical so that Facebook advertises the items someone has purchased to strangers, with a note that provides her name and says she has purchased the items. This situation is more difficult. The difference lies in how a user conceives of Facebook. The website exists for the purpose of sharing information about your life with the outside world, but Facebook leads users to believe that with the right privacy setting, only a users' "friends" can see information about them. Because Facebook sets up this expectation, it would be a violation of the resulting trust for Facebook to share purchase information with a non-friend (that is to say, someone whom the user has not approved for access to their posts). The average Facebook user expects that when they have the option to adjust privacy settings so that only friends can view their information, the website will act in accordance with those settings.

c) Uber Uses Data To Embarrass a Critic

In 2014, an Uber executive suggested—perhaps off-handedly—that in order to fight negative press stories accusing Uber of sexism and misogyny, Uber should hire opposition researchers and use the data it has about a particular journalist to “give the media a taste of its own medicine.”¹⁵² Uber's then-CEO, Travis Kalanick, maintained that this was a departure from Uber's “values and ideals,”¹⁵³ but the suggestion is interesting—could it do this and remain within a fiduciary duty?

149. One such notification reads, “This app may post on your behalf, including radio stations you joined, songs you played and more.” Whitson Gordon, *Understanding OAuth: What Happens When You Log into a Site with Google, Twitter or Facebook*, LIFEHACKER (June 13, 2012, 1:00 PM), <https://lifehacker.com/5918086/understanding-oauth-what-happens-when-you-log-into-a-site-with-google-twitter-or-facebook> [<https://perma.cc/VU8S-UWM3>].

150. See Part IV for further discussion on shifting user expectations.

151. There is also a question about manipulation here—is it manipulative to use my friends to advertise to me? However, this is the kind of practice with which consumers are familiar. It is essentially an even more sophisticated level of targeted advertising, but users likely understand what is happening and do not lose autonomy when it occurs.

152. Ben Smith, *Uber Executive Suggests Digging Up Dirt On Journalists*, BUZZFEED (Nov. 17, 2014, 4:57 PM), www.buzzfeed.com/bensmith/uber-executive-suggests-digging-up-dirt-on-journalists [<https://perma.cc/CN3K-MPAP>].

153. Josh Constine, *Uber CEO Says Exec's Threats To Journalists "Showed A Lack Of Humanity" But Doesn't Fire Him*, TECHCRUNCH (Nov. 18, 2014), <https://techcrunch.com/2014/11/18/emil-michael-thrown-under-the-uber> [<https://perma.cc/KK4F-RVD6>].

Consider a case in which Uber targets a particular critic and looks through the data they have gathered through the journalist's use of the service. Uber finds that she is married with two children, and lives with her husband and family in Brooklyn. However, her Uber data shows her leaving work, going to the same Upper West Side apartment several nights a week, and then heading back to her own home after a few hours. This, paired with data that shows the apartment belongs to a male work associate of hers, could suggest she is having an affair. The next time the journalist writes a column criticizing Uber, Uber responds with a blog post describing her affair in an effort to discredit her.

Assuming Uber is targeting the one journalist and not a specific class of people, its actions do not violate the principle of antidiscrimination. But this would violate the third-party principle through the sharing of data in a completely unexpected way. While Uber is not releasing a spreadsheet of data, it is presenting the user's data (i.e., the journalist's ride history) in a public story about her. Under no circumstance would a reasonable user expect her data to be used in this way.

Additionally, Uber is using her data to manipulate her in two ways. If the story is published on Uber's blog, it is manipulative first because Uber is attempting to covertly push an agenda—one that is aimed at discrediting a journalist.¹⁵⁴ If someone from Uber publishes the story without attaching Uber's name, the increased covertness makes it more manipulative. Second, this is a usage of a user's data to maximize the company's own welfare by bringing down a critic, at the expense of the journalist's privacy and reputation. As such, this kind of behavior crosses multiple lines which violate the fiduciary duty. To be clear, it is the usage of the data, which the user provided to Uber to facilitate a specific service that makes this action a violation of Uber's fiduciary duty. If Uber had merely written a blog post discrediting the journalist by pointing to other stories she had written, picking on her lackluster education, or just fabricating lies, it would not violate its informational fiduciary duty because it would not be using information it possessed by virtue of the journalist having used Uber's service.

D. VIOLATING THE COMPANY'S OWN PRIVACY POLICY

The final principle, which prohibits firms from violating their own privacy policies, does not just define a fourth aspect of the information fiduciary duty. It also illuminates the underlying assumption of the information fiduciary duty itself—that users' reasonable expectations mark the ultimate limit on data privacy practices. Thus, if practices are brought within users' expectations or are predictable to a reasonable user, the practice will not violate the fiduciary

154. This violation might be remedied if the story makes clear that this journalist has been critical of Uber—the agenda-pushing would no longer be covert.

duty. As mentioned in Section II.A, the FTC routinely uses its Section 5 authority to hold companies accountable to the standards they set for themselves in their privacy policies. But ultimately, companies should not be able to set their own standards—there should be some baseline to which every service provider is held.¹⁵⁵ Though the FTC is empowered to bring enforcement actions based on the policies,¹⁵⁶ baseline standards are needed.

Most companies' privacy policies discuss with whom data may be shared. The policies vary widely, but almost all allow some sort of sharing with other companies. Notably, the typical privacy policy highlights sharing, but not internal company practices. This indicates that service providers may not believe they should have to disclose to users how they use data internally or what practices they will and will not implement.¹⁵⁷

155. Of course, firms should be permitted to provide *more* protection that the information fiduciary baseline.

156. 15 U.S.C. § 45 (2012); *see also supra* Section II.A.

157. Walmart, which claims it “cares deeply about maintaining the trust and confidence that our customers place in us,” *Responsible Disclosure Policy*, WALMART, <https://corporate.walmart.com/article/responsible-disclosure-policy> [<https://perma.cc/PJ9Y-8HA6>] (last visited Feb. 28, 2018), says only that the company “will not sell or rent your personal information” but may “share your personal information in limited circumstances, such as to conduct our business, when legally required, or with your consent.” *Walmart Privacy Policy*, WALMART (Nov. 2017), <http://corporate.walmart.com/privacy-security/walmart-privacy-policy> [<https://perma.cc/RVD5-ADLA>].

Uber's policy says that it may share information with: (1) drivers; (2) other riders if a ride-sharing service is used; (3) other people as directed by the user; (4) the general public if the user submits content in a public forum; (5) the owner of Uber accounts that someone uses (i.e., their employer); (6) Uber subsidiaries, affiliates, service providers, and business partners; (7) “law enforcement officials, government authorities, or other third parties as necessary to enforce our Terms of Service, user agreements, or other policies, to protect Uber's rights or property or the rights or property or others”; (8) third parties to provide a service requested by the user through a partnership or promotional offering; (9) Uber “vendors, consultants, marketing partners, research firms, and other service providers or business partners”; (10) in connection with or during merger negotiations; or (11) if consent is given. UBER, *supra* note 134.

Google's privacy policy maintains that it does not share personal information outside Google unless: (1) they have the user's consent, which is opt-in for sensitive personal information; (2) the information is being shared with domain administrators; (3) the information is being shared for external processing; or (4) the information is being shared for legal reasons. The policy further articulates that Google may share non-personally identifiable information with “partners,” which includes publishers, advertisers, and connected sites. *Privacy Policy*, GOOGLE, <https://www.google.com/policies/privacy> [<https://perma.cc/56MF-W2L6>].

Facebook's policy says it shares information with: (1) “people you share and communicate with”; (2) people that see content others share about you; (3) apps, websites, and third-party integrations on or using Facebook's services; (4) Facebook companies; and (4) a new owner,

1. *An Information Fiduciary's Privacy Policy*

An information fiduciary must comply with the restrictions it imposes on itself, because that is the promise it has made to its users. But a user's expectations of a company can be shifted through clear disclosures.¹⁵⁸ When a company makes a promise in its privacy policy, such as that it “will not sell or rent your personal information,”¹⁵⁹ it must not violate that promise. As discussed, the FTC and CFPB have sued companies for misrepresentation when they have violated their own privacy policies.¹⁶⁰ One could argue that a user's expectations cannot be based on privacy policies, since users never read them. However, if the fiction works in *favor* of service providers, in that they are allowed to continue various practices if they have “disclosed” them, the fiction should also be extended to protect users.

But in an ideal (and hopefully not-too-distant) world, privacy policies could be one to two pages, and easy to read and comprehend.¹⁶¹ In that case, it is even more important that companies abide by their own policies since users may actually be able to make informed decisions when engaging with a company. An information fiduciary should be required to provide clear disclosures that identify the company's data privacy policies in plain language. Key practices might be those which are most pervasive or those which are least predictable. A good model is the CFPB's “Know Before You Owe” mandatory one-page disclosure for mortgage loans.¹⁶² The CFPB performed research for

if an acquisition were to occur. Additionally, though, Facebook shares non-personally identifiable information with “advertising, measurement, and analytics services” and vendors, service providers, and “other partners who globally support our business.” *Data Policy*, FACEBOOK, <https://www.facebook.com/policy.php> [<https://perma.cc/Q64D-FF4T>] (last visited Feb. 28, 2018).

158. This also indicates that one of the previous four mandates can be circumvented through clear disclosure.

159. *Walmart Privacy Policy*, WALMART, *supra* note 157.

160. *See, e.g.*, Press Release, Fed. Trade Comm'n, Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices (Dec. 20, 2016), <https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively> [<https://perma.cc/4V5T-VW3B>].

161. *Cf.* KLEIMANN COMM'N GRP., INC., KNOW BEFORE YOU OWE: QUANTITATIVE STUDY OF THE CURRENT AND INTEGRATED TILA-RESPA DISCLOSURES (2013), https://s3.amazonaws.com/files.consumerfinance.gov/f/201311_cfpb_study_tila-respa_disclosure-comparison.pdf [<https://perma.cc/LZB6-KA5K>] (describing the development of the CFPB's mortgage disclosure rules); KLEIMANN COMM'N GRP., INC., KNOW BEFORE YOU OWE: EVOLUTION OF THE INTEGRATED TILA-RESPA DISCLOSURES (2012), https://s3.amazonaws.com/files.consumerfinance.gov/f/201207_cfpb_report_tila-respa-testing.pdf [<https://perma.cc/5PJL-KU5G>] (describing the study that informed the drafting of the mortgage disclosure form design).

162. *See Know Before You Owe: Mortgages*, CONSUMER FIN. PROT. BUREAU 1 (Nov. 20, 2013), http://files.consumerfinance.gov/f/201311_cfpb_factsheet_kbyo_mortgage-disclosures.pdf

over two years to determine how to make disclosures most helpful to consumers.¹⁶³ Information fiduciaries should provide a similar type of form rather than the thousands of words of small, light grey text that many provide now. This would allow a user to understand how their data might be used and decide accordingly whether to hand over their information. To be sure, service providers should not be able to disclaim certain duties, such as the duty not to covertly manipulate, but they could notify users of other practices and allow users to then decide for themselves about whether they want to use the service.

2. *Hypothetical: Facebook Pushes a Political Agenda, Part II*

Think back to an early hypothetical, in which Facebook pushed a political agenda on users. What if when users signed up for the service Facebook disclosed that it may push its political agenda on users? Or if Facebook sent every current user an email alerting them to the implementation of a new practice? This might make it consistent with the fiduciary duty. The reason that manipulation of a user's autonomy is unacceptable is because it is covert, so users cannot respond to it rationally and consciously. If Facebook tells users that it will try to get them to vote a certain way, the "manipulation" is now more like targeted advertising—the user is able to respond to it.

A natural reaction to this might be that people stop using Facebook. But would they? Facebook's network effects are immense; many users might just go along with it, as they have with a number of companies that have publicly implemented unsavory policies. As Albert Hirschman explains, users can respond to a company's change in policies in two ways: exit or voice.¹⁶⁴ If exit is difficult, users can respond with voice. And the decision between these two options will be affected by how loyal the user feels to the company.¹⁶⁵

[<https://perma.cc/47TK-57XF>] (hereinafter CFPB, *Mortgages*) ("The two new forms, one which consumers will receive shortly after applying for a loan and one which they will receive shortly before closing, use plain language and design to make it easier for consumers to locate key information such as the interest rate, monthly payments, and the costs to close the loan."); see also *How We Improved the Disclosures*, CONSUMER FIN. PROT. BUREAU, <https://www.consumerfinance.gov/know-before-you-owe/compare> [<https://perma.cc/QGU4-4YGP>] (last visited Feb. 28, 2018).

163. CFPB, *Mortgages*, *supra* note 162, at 2.

164. See generally ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970). "Exit" represents the idea that, when management has "failed," consumers can stop buying the firm's products, causing revenue to drop. *Id.* at 4. The other option that consumers can use to express displeasure, "voice," occurs through "general protest addressed to anyone who cares to listen." *Id.*

165. *Id.* (explaining that were loyalty is lacking, people would be more likely to choose exit over voice).

Exit and voice have worked for users in this space. For example, in 2012, Instagram changed its policy to claim the right to sell users' photos.¹⁶⁶ Within two days, there was so much backlash that Instagram retreated from the policy.¹⁶⁷ So Facebook—or any other service provider—does have the option to push an agenda if it is out in the open, and they may or may not risk user exit. And smaller companies with fewer network effects may simply have to implement a privacy policy that is acceptable to its potential users.

IV. ENFORCING THE INFORMATION FIDUCIARY DUTY

Simply defining practices that may or may not be consistent with an information fiduciary duty is not enough. There are two main paths forward from here—one involving legal changes and the other involving industry changes. On the legal side, two steps must be taken to make the information duty a reality: (1) a federal statute that imposes the duty on service providers, and (2) enforcement in courts.¹⁶⁸ While this Article does not purport to lay out a new statutory scheme in its entirety, it briefly sketches out what this might look like in practice.

The statute would define this duty and categorize who is subject to it. The main task would be to define “service provider” to state clearly who must abide by the information fiduciary duty. Coverage should be clear and predictable for industry. Ideally, it would cover any company that collects user data and stores it beyond the conclusion of each transaction, with some sort of exception for firms that serve a small number of users.¹⁶⁹ But outside of defining the category of covered entities and the general duty, the statute should be general. Courts could define its contours as cases arise by determining what a “reasonable user” should expect. The duty itself is based on users' expectations, which will shift as data collection practices, artificial

166. See Joshua Brustein, *Anger at Changes on Instagram*, N.Y. TIMES (Dec. 18, 2012, 4:05 PM), <https://bits.blogs.nytimes.com/2012/12/18/anger-at-changes-on-instagram> [<https://perma.cc/26W9-8U5Z>].

167. See Harold Maass, *Instagram's Privacy Policy Retreat: Too Late?*, WEEK (Dec. 21, 2012), <https://theweek.com/articles/469195/instagrans-privacy-policy-retreat-late> [<https://perma.cc/VR42-UJFV>]; see also Nicole Perloth & Jenna Wortham, *Instagram's Loss Is a Gain for Its Rivals*, N.Y. TIMES (Dec. 20, 2012, 10:00 PM), <https://bits.blogs.nytimes.com/2012/12/20/instagrans-loss-is-other-apps-gain> [<https://perma.cc/ATJ4-Z58C>].

168. States could do this as well but because of the complications stemming from data territoriality and the fact that many service providers serve consumers in all fifty states, a federal regime would be more predictable for users and service providers alike.

169. This would likely require a study to determine what constitutes a “small business” in the online service provider and data collection space, but should end up falling in line with other small business exceptions, to avoid undue burden.

intelligence, and the Internet of Things continue to develop and change the way users interact with technology and the world more broadly.

A broad statute that allows courts to easily adapt it to users' changing expectations is not as unpredictable as it sounds. A statute should define the fiduciary duty as maintaining data collection and usages practices that are consistent with a reasonable user's expectations. Judges are well-versed in defining the "reasonable person," and juries are asked to do it all the time.¹⁷⁰ Consider a hypothetical lawsuit against Facebook for manipulating users by pushing a political agenda. A judge or jury would look at all of the facts and determine whether a reasonable user should have expected this manipulation.

The proposed California Consumer Privacy Act of 2018 is an interesting model for this kind of legislation.¹⁷¹ While it does not specifically propose a fiduciary duty, it takes a number of steps to level the playing field between users and service providers such that users have the ability to understand more fully how data is collected and used. For example, it requires businesses to disclose what personal information it has collected to individual consumers upon request¹⁷² and gives users the right to prevent businesses from selling their personal information.¹⁷³

Once a fiduciary duty is legally imposed, it could be enforced privately or publicly. California's proposed law provides for both avenues.¹⁷⁴ The concern with private enforcement would be defining an injury-in-fact such that the threat of private litigation has an effect on companies' behavior.¹⁷⁵ It is a viable mechanism, but public enforcement is likely a stronger tool. The FTC and state agencies should be given an active role in enforcing this law to ensure that it does not go unenforced simply because of standing doctrine.

170. *See, e.g.*, *People v. Jefferson*, 14 Cal. Rptr. 3d 473, 481 (Cal. Ct. App. 2004) ("The jury must consider defendant's situation and knowledge, which makes the evidence relevant, but the ultimate question is whether a reasonable person, not a reasonable battered woman, would believe in the need to kill to prevent imminent harm."); *State v. Morgan*, 648 N.W.2d 23, 32–33 (Wis. Ct. App. 2002) (defining the reasonable person in the context of *Miranda* analysis); *Radtke v. Everett*, 501 N.W.2d 155, 166 (Mich. 1993) (defining the standard and maintaining that "the reasonable person standard is sufficiently flexible . . . without destroying the vital stability provided by uniform standards of conduct"); *see also* Alan D. Miller & Ronen Perry, *The Reasonable Person*, 87 N.Y.U. L. REV. 323 (2012) (arguing that normative definitions of the "reasonable person" are preferable to positive definitions).

171. THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018, VERSION 2 (Oct. 12, 2017), <https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf> [<https://perma.cc/HK5A-S6NM>].

172. *Id.* § 1798.101.

173. *Id.* § 1798.102.

174. *Id.* §§ 1798.108 to 1798.109.

175. This is the subject of much debate, *see, e.g.*, *Spokeo v. Robins*, 136 S. Ct. 1540 (2016), but is outside the scope of this Article.

But while the law should impose this duty, the beauty of the fiduciary duty lies in the ability to shift user expectations. An additional step that should be taken is for companies to take privacy policies more seriously—not just as a liability issue, but as an opportunity. Rather than bury provisions in thousands of words of small, light grey text, companies could produce one-page policy summaries that define key terms and describe data practices. By doing so, a “reasonable user’s” expectations should shift, and the company can test or implement new practices. By allowing users a meaningful chance to opt in or out, companies could allow them to act autonomously and see what users are willing to allow. Companies should enable their users to engage with them on equal footing so that ultimately, users can make informed decisions about how they share their data.

V. CONCLUSION

The United States has a long way to go in terms of mandating protections for users’ personal information. Holding service providers to an information fiduciary standard is a viable way to ensure that data-focused business models can continue to function while individuals are adequately protected. The four principles outlined here—anti-manipulation, antidiscrimination, limited third party sharing, and holding companies to their own privacy policies—all focus on user expectations. And as new technologies emerge and old tools morph into something new, user expectations may change.

As Justice Sotomayor noted in 2012, “[p]erhaps . . . some people may find the tradeoff of privacy for convenience worthwhile, or come to accept this diminution of privacy as inevitable, and perhaps not.”¹⁷⁶ As people become more comfortable with emerging technologies, their “reasonable expectations” may shift. But shifting expectations should not be an excuse for a complete lack of privacy standards for firms. There can be a tradeoff that works for the service provider and the user, and if the standard is based in reasonableness, it can evolve alongside technology. Abiding by fiduciary principles will help service providers be the trustworthy entities they hold themselves out to be, ensuring that the era of Big Data does not necessarily mean the end of personal privacy.

176. *United States v. Jones*, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (internal quotations omitted).

COMPUTER-AIDED DESTRUCTION: REGULATING 3D-PRINTED FIREARMS WITHOUT INFRINGING ON INDIVIDUAL LIBERTIES

Jessica Berkowitz[†]

ABSTRACT

Additive manufacturing, also known as 3D printing, is a rapidly developing technology that is changing the way people manufacture goods. Individual consumers can purchase a 3D printer for their own personal use, providing them with the ability to create fully customizable products in the privacy of their own homes. However, there is one 3D-printed product that is causing much controversy and debate: firearms. Armed with a 3D printer and the desired design and filament, an individual can print a fully functioning weapon, bypassing federal and state licensing, registration, and manufacturing requirements. There are statutes currently in effect that may offer some control over 3D-printed guns; however, these statutes may need to be altered to provide adequate regulatory control over illegal possession and misuse of 3D-printed firearms. Additionally, any future regulations will almost certainly be scrutinized under both the First and Second Amendments, balancing public safety concerns with individual liberties. Moreover, many possible regulations of the technology itself would be impractical and run afoul of the public policy goal of protecting technological innovation. It is currently—and will likely always be—impossible to 3D-print gunpowder, a necessary component of a functioning firearm. Therefore, to best regulate 3D-printed firearms, while also protecting constitutional liberties and technological innovation, this Note proposes an expansion of the Brady Bill to require background checks for ammunition purchases. This is the most readily available remedy to the specific regulatory challenges posed by 3D-printed firearms, as amending the Brady Bill is relatively simple and less invasive for firearms dealers who already have access to the National Instant Criminal Background Check System used for firearms purchases.

DOI: <https://doi.org/10.15779/Z38BG2H96S>

© 2018 Jessica Berkowitz.

[†] Juris Doctor Candidate, Vanderbilt University Law School 2018. Thank you to the *Berkeley Technology Law Journal* for selecting my Note as part of its 2017 Writing Competition, with particular thanks to the editors for their beneficial feedback throughout the editing process. I would also like to thank the *Vanderbilt Law Review* staff for their initial guidance in the note-writing process. Most importantly, thank you to my husband who first posed the question, “Are 3D-printed firearms even legal?!” and without whose support I could not have done this.

TABLE OF CONTENTS

I.	INTRODUCTION	53
II.	READY, PRINT, FIRE!: THE BASICS OF 3D PRINTING AND 3D-PRINTED FIREARMS	55
A.	ADDITIVE MANUFACTURING	56
B.	3D PRINTING A FUNCTIONING FIREARM	58
C.	DEFENSE DISTRIBUTED AND THE FIRST 3D-PRINTED HANDGUN	60
D.	<i>DEFENSE DISTRIBUTED V. U.S. DEPARTMENT OF STATE</i>	63
III.	STARING DOWN THE BARRELL: SCRUTINIZING 3D- PRINTED GUNS UNDER CURRENT LAW	64
A.	THE CURRENT GUN CONTROL REGULATORY SCHEME AND ITS INABILITY TO REGULATE 3D-PRINTED FIREARMS	64
1.	<i>The Undetectable Firearms Act of 1988</i>	66
2.	<i>Arms Export Control Act of 1976 and the International Traffic in Arms Regulation</i>	67
3.	<i>The National Firearms Act of 1934, the Gun Control Act of 1968, and the Brady Handgun Prevention Act of 1993</i>	69
B.	CONSTITUTIONAL BARRIERS TO REGULATION: THE FIRST AND SECOND AMENDMENT	72
1.	<i>The First Amendment</i>	72
2.	<i>The Second Amendment</i>	75
IV.	TAKING AIM: ACHIEVING EFFECTIVE LEGISLATION	78
A.	THE CASE AGAINST REGULATING 3D PRINTING TECHNOLOGY	78
B.	REGULATING GUNPOWDER	81
V.	CONCLUSION	84

I. INTRODUCTION

Additive manufacturing, more commonly known as three-dimensional (“3D”) printing, is a rapidly developing technology that presents novel legal challenges. One of the most difficult challenges is how to adequately regulate 3D-printed firearms.¹ Anyone with a 3D printer can now turn a digital blueprint into a functioning lethal weapon, bypassing numerous federal gun control laws.² Although 3D-printing technology has existed since the 1980s, technological advances and decreasing costs have made these printers more accessible to individual consumers.³ Because the market for 3D printers is relatively new, it is not yet directly regulated, nor has the Supreme Court had an opportunity to address the legal implications of 3D-printed products.⁴ As 3D printers become more available to the public, there is concern many people may use the technology to circumvent the law.⁵

Armed with a 3D printer and Internet access, individuals may manufacture firearms in their own homes, thereby avoiding licensing, registration, manufacturing, and background check requirements.⁶ Currently, very few laws exist that can regulate the possession or manufacture of 3D-printed firearms,

1. For the purposes of this Note, “3D-printed firearms” include any firearm that is made with any 3D-printed part that contributes to the firearm’s functionality, regardless of the material from which it is made. See Caitlyn R. McCutcheon, Note, *Deeper Than a Paper Cut: Is It Possible to Regulate Three-Dimensionally Printed Weapons or Will Federal Gun Laws Be Obsolete Before the Ink Has Dried?*, 2014 U. ILL. J.L. TECH. & POL’Y 219, 222.

2. See *id.* at 221.

3. See *id.* at 220, 223.

4. See *id.* at 222; Jennifer Huddleston Skees, *What a Supreme Court Decision on Cheerleading Uniforms Means for the Future of 3D Printing*, PLAIN TEXT (Aug. 2, 2017), <https://readplaintext.com/what-a-supreme-court-decision-on-cheerleading-uniforms-means-for-the-future-of-3d-printing-ad086e6b0469> [<https://perma.cc/9PRE-R7HH>].

5. See, e.g., McCutcheon, *supra* note 1, at 221; Christopher J. Ferguson, *3-D Printed Guns Are a Boon for Criminals*, CNN (May 7, 2013, 7:28 AM), <http://www.cnn.com/2013/05/07/opinion/ferguson-printable-gun/> [<https://perma.cc/TVR6-G5XR>] (expressing concern that 3D-printed guns could be used to “circumvent existing” prohibitions on gun possession); Andy Greenberg, *Bill to Ban Undetectable 3D Printed Guns Is Coming Back*, WIRED (Apr. 6, 2015, 7:00 AM), <https://www.wired.com/2015/04/bill-ban-undetectable-3-d-printed-guns-coming-back/> [<https://perma.cc/A883-EDEW>] (describing congressional legislation proposing a ban on 3D-printed guns); Jordan Pearson, *A 3D Printing Company Is Trying to Deny Legal Protection to Hobbyists*, VICE: MOTHERBOARD (May 1, 2015, 2:14 PM), https://motherboard.vice.com/en_us/article/ypw4by/the-legal-fight-to-put-whatever-you-want-in-a-3d-printer [<https://perma.cc/Y422-GD6F>] (discussing the controversy over a law that “make[s] tampering with products that have digital protections in place against the law, whatever the eventual goal” in the context of 3D printing).

6. See McCutcheon, *supra* note 1, at 221.

as long as an individual does not sell, trade, share, or cross state lines with such weapons.⁷ Thus far, 3D-printed firearms have mostly raised intellectual property issues, including concerns over patent, trademark, and copyright infringement.⁸ However, as the technology becomes more prevalent, it will undoubtedly frustrate current gun control efforts.⁹

Although some existing gun control statutes may encompass 3D-printed firearms, these laws do not sufficiently control for the novel challenges arising from the use of 3D-printing technology.¹⁰ For example, 3D-printed guns made from plastic may circumvent the Undetectable Firearms Act's ban on firearms that cannot be detected by metal detectors.¹¹ Similarly, individuals who print, instead of purchase, firearms may bypass background checks mandated under the Brady Handgun Violence Prevention Act, opening firearm access to prohibited classes.¹² Potential regulations regarding 3D-printed guns may also implicate First and Second Amendment challenges. The digital blueprints necessary to create 3D-printed products likely constitute electronic speech, so any gun-specific regulation of these files would be subject to strict scrutiny in court.¹³ Furthermore, the Second Amendment protects an individual's right to self-manufacture firearms, which likely extends to homemade 3D-printed guns.¹⁴ The Supreme Court seemingly agrees that the right to print one's own gun is protected under both the First and Second Amendments, making a future ban on 3D-printed firearms unlikely.¹⁵

With tens of thousands of gun-related homicides per year,¹⁶ 3D-printing firearms must be scrutinized in light of its capability to add to that number. Currently, the likelihood of countless individuals printing their own guns is low, but 3D printers will generally contribute to placing more illegal guns into the market and provide criminals with a new avenue to obtain firearms.¹⁷

7. See Elizabeth A. Harlan, *The Inadequacy of the Second Amendment for 3D Printed Guns*, 48 MD. B.J. 25, 30 (2015).

8. See McCutcheon, *supra* note 1, at 220.

9. See *id.*

10. See *infra* Section III.A.

11. See 18 U.S.C. § 922(p) (2012); Harlan, *supra* note 7, at 30 (“[I]t is inevitable that other plastic 3D guns manufactured at home will not include any metal parts.”).

12. See 18 U.S.C. § 922(g) (2012) (listing prohibited classes).

13. See Josh Blackman, *The 1st Amendment, 2nd Amendment, and 3D Printed Guns*, 81 TENN. L. REV. 479, 499–501 (2014).

14. See McCutcheon, *supra* note 1, at 237–38; *infra* Section III.B.2.

15. See *District of Columbia v. Heller*, 554 U.S. 570, 625–29 (2008); Blackman, *supra* note 13, at 492.

16. See Rory K. Little, *Guns Don't Kill People, 3D Printing Does? Why the Technology Is a Distraction from Effective Gun Controls*, 65 HASTINGS L.J. 1505, 1506 (2014).

17. See McCutcheon, *supra* note 1, at 237.

Furthermore, inexperienced users may harm themselves in attempting to print and shoot a poorly designed firearm. It is vital, however, that lawmakers are careful not to allow the novelty of 3D printing to distract from the actual issue at hand: effective gun control.¹⁸

This Note analyzes how 3D-printed firearms fit into current gun control regulations and modern First and Second Amendment jurisprudence. It further proposes a solution as to how the legal system can regulate 3D-printed guns, with minimal infringement on individuals' constitutional rights. Part II provides background on why 3D printing is important to innovation, how the technology works, and how individuals may use it to self-manufacture firearms. Part III discusses why the current regulatory scheme may not effectively control 3D-printed guns and analyzes the constitutional hurdles to possible regulation. Part IV proposes extending current federal firearms requirements to ammunition purchases, which would help curtail the number of illegally possessed guns made with 3D printers while also protecting innovation of the technology. Finally, Part V concludes, reiterating that regulating ammunition is the most readily available approach to controlling 3D-printed firearms while preserving individual liberties.

II. READY, PRINT, FIRE!: THE BASICS OF 3D PRINTING AND 3D-PRINTED FIREARMS

In 2013, President Barack Obama described 3D printing as having “the potential to revolutionize the way we make almost everything.”¹⁹ Additive manufacturing is already transforming numerous industries: for instance, NASA utilized the technology to create parts for its spacecrafts.²⁰ Moreover, in the medical field, 3D printers are used every day to create devices such as hearing aids, prosthetics, orthopedic implants, and dental fillings.²¹ With this technology, surgeons can even print replicas of a patient's body to practice surgery before it is performed.²²

The technology allows for a nearly effortless manufacturing process that is more efficient and less wasteful than traditional methods.²³ In 2012, the federal

18. See Little, *supra* note 16, at 1510 (asserting that regulations should focus on the misuse of technology and not inhibit innovation).

19. Blackman, *supra* note 13, at 483.

20. See McCutcheon, *supra* note 1, at 221.

21. See Peter Jensen-Haxel, Comment, *3D Printers, Obsolete Firearm Supply Controls, and the Right to Build Self-Defense Weapons Under Heller*, 42 GOLDEN GATE U.L. REV. 447, 451–52 (2012) (describing dental filling production).

22. See *id.*

23. See McCutcheon, *supra* note 1, at 222.

government dedicated thirty million dollars to the National Additive Manufacturing Innovation Institute to increase American manufacturing jobs related to 3D printing.²⁴ However, many commenters are concerned that as the use of 3D-printing technology becomes widespread, some individuals will use it to further illegal enterprises.²⁵ The ability to regulate 3D-printed guns effectively is at the forefront of this concern.²⁶

A. ADDITIVE MANUFACTURING

Additive manufacturing consists of a layering process, adding layer by layer of raw material until the desired object is complete.²⁷ An operating printer resembles a sort of robotic hot glue gun, but instead of glue, the printer emits whatever filament with which it is loaded.²⁸ Although plastic is the most common filament,²⁹ different types of printers can print objects using a wide variety of materials, including metals like titanium and gold, and even edible materials such as sugar.³⁰ These printers can print more complex shapes and structures than are possible through traditional manufacturing.³¹ Unlike other manufacturing methods such as cutting or injection molding, 3D printing requires only one machine, which does not need to be reconfigured before a different object is created.³² It is also significantly more efficient than other forms of manufacturing because it can preassemble the product.³³

24. See Anne Lewis, *The Legality of 3D Printing: How Technology Is Moving Faster than the Law*, 17 TUL. J. TECH. & INTELL. PROP. 303, 304 (2014).

25. See, e.g., Brian Krebs, *Gang Used 3D Printers for ATM Skimmers*, KREBS ON SECURITY (Sept. 20, 2011), <https://krebsonsecurity.com/2011/09/gang-used-3d-printers-for-atm-skimmers/> [<https://perma.cc/E797-9PN2>] (providing an example of how criminals have used 3D-printing technology to commit crimes); see also *supra* note 6 and accompanying text.

26. See McCutcheon, *supra* note 1, at 235–37.

27. See *id.* at 222–23.

28. See A. J. Jacobs, *Dinner Is Printed*, N.Y. TIMES (Sept. 21, 2013), www.nytimes.com/2013/09/22/opinion/sunday/dinner-is-printed.html [<https://perma.cc/UJ4E-NB9C>].

29. See Jeff Yoders, *What Materials Are Used in 3D Printing? It's More Fantastic Than Plastic*, REDSHIFT (Nov. 4, 2014), <https://www.autodesk.com/redshift/what-materials-are-used-in-3d-printing/> [<https://perma.cc/H243-D5DB>] (“Plastic still reigns supreme in the 3D-printing materials world.”); Elizabeth Palermo, *Fused Deposition Modeling: Most Common 3D Printing Method*, LIVE SCI. (Sept. 19, 2013, 6:28 PM), <https://www.livescience.com/39810-fused-deposition-modeling.html> [<https://perma.cc/V7NU-A3XQ>] (noting that Fused Deposition Modeling is the most common form of 3D printing, which uses a plastic filament).

30. See Jensen-Haxel, *supra* note 21, at 448. Other materials include rubber, hard plastics, temperature resistant materials, opaque, transparent materials, and stainless steel. McCutcheon, *supra* note 1, at 225.

31. See McCutcheon, *supra* note 1, at 222.

32. See Jensen-Haxel, *supra* note 21, at 450.

33. See *id.* at 450–51. For example, a 3D-printed clock will print with all the gears already inside. *Id.*

To begin, one must have a computer-aided design (“CAD”) file, which acts as a digital blueprint for the desired object.³⁴ CAD software requires some level of expertise, particularly for complex designs.³⁵ However, for beginners, there are numerous resources online to bypass creating one’s own CAD files, including software tutorials and thousands of existing downloadable files.³⁶ For example, websites such as Thingiverse.com and GrabCAD.com host online communities of millions of skilled designers who upload and share their own CAD creations for free.³⁷

Although 3D printers are more prevalent in commercial settings, they are growing in popularity among private consumers, who can purchase the technology at stores like Home Depot and Best Buy.³⁸ As of this writing, Amazon offers a “mini” 3D printer for only \$199.99.³⁹ This model, advertised as “[a]ffordable 3D printing for everyone,” is a nine-pound desktop printer that works with “any type of filament,” including metal.⁴⁰ Other companies lease printers or, for a small fee, will print any design and ship it to the consumer.⁴¹ Some economists predict that the 3D-printing market will become a \$6.5 billion industry by 2019, and increase by 300 percent in 2020.⁴² As mainstream awareness continues to grow, 3D-printing costs are expected to further decrease, providing users an inexpensive and convenient way to produce physical objects from their home computers.⁴³

Moreover, the manufacturing industry can be completely transformed by the numerous benefits of 3D printing.⁴⁴ The technology is likely cheaper than

34. See McCutcheon, *supra* note 1, at 223.

35. See *id.*

36. *Def. Distributed v. U.S. Dep’t of State*, 838 F.3d 451, 454–55 (2016).

37. See GRABCAD, <https://grabcad.com/> [<https://perma.cc/WS3W-EMVX>] (last visited Mar. 12, 2018); THINGIVERSE, <https://www.thingiverse.com/> [<https://perma.cc/Q6JZ-G6U4>] (last visited Feb. 12, 2017).

38. See *Def. Distributed*, 838 F.3d at 454.

39. *Monoprice 115365 Select Mini 3D Printer with Heated Build Plate, Includes Micro SD Card and Sample PLA Filament*, AMAZON, <https://www.amazon.com/Monoprice-Select-Printer-Heated-Filament/dp/B01FL49VZE/> [<https://perma.cc/2HEK-3C9G>] (last visited Mar. 12, 2018).

40. *Id.*

41. Becoming 3D and Stratasys are examples of companies that lease 3D printers. *3D Printer Leasing*, BECOMING 3D, <https://www.becoming3d.com/3d-printer-leasing/> [<https://perma.cc/PWF7-RVMB>] (last visited Mar. 12, 2018); STRATASYS, <http://www.stratasys.com/> [<https://perma.cc/ZCB9-9QZS>] (last visited Mar. 12, 2018).

42. See McCutcheon, *supra* note 1, at 224.

43. See *id.* at 220, 223.

44. See THOMAS CAMPBELL ET AL., ATLANTIC COUNCIL, COULD 3D PRINTING CHANGE THE WORLD? TECHNOLOGIES, POTENTIAL, AND IMPLICATIONS OF ADDITIVE MANUFACTURING 1–2 (2011), http://www.atlanticcouncil.org/images/files/publication_pdfs/403/101711_ACUS_3DPrinting.PDF [<https://perma.cc/BF8D-XJ4Q>].

traditional manufacturing methods and can allow for quick production, reducing product to market time.⁴⁵ Due to its ability to print complex shapes and structures, there is potential for practically unlimited concept and design development, leading to better quality products and more customization.⁴⁶ It produces less waste than traditional manufacturing, is more sustainable, and is expected to reduce both export reliance and surplus by localizing production.⁴⁷

The technology provides numerous benefits, but also boundless opportunities for abuse. One technology expert has predicted that within the next decade, the majority of American households will own a 3D printer.⁴⁸ Troublingly, 3D printers have already been used to further illegal endeavors.⁴⁹ For example, a gang used a 3D-printed skimmer to steal \$400,000 from an ATM.⁵⁰ Because this is quickly developing technology, it may be better to prepare for potential issues now before 3D printing becomes a widespread legal nightmare.⁵¹ In particular, 3D-printed weapons are able to evade current gun control regulations because they may be undetectable, untraceable, and easily disposed of.⁵² Because the technology allows anyone to print an almost fully functioning, deadly weapon in the person's own home, it is especially prudent to address regulatory issues now.⁵³

B. 3D PRINTING A FUNCTIONING FIREARM

Gunsmiths and hobbyists have taken advantage of 3D printing's unique manufacturing benefits and have begun to perfect the ability to print a fully functioning firearm.⁵⁴ A mere two years after the first attempt, the concept of printing an operable gun became a reality.⁵⁵ In 2013, a 3D-printed firearm, made up of almost completely printed parts, shot 600 rounds of ammunition.⁵⁶

45. *See id.* at 10.

46. *See id.* at 5–6.

47. *See id.* at 2, 6.

48. *See* Lewis, *supra* note 24, at 307.

49. *See* McCutcheon, *supra* note 1, at 235; Krebs, *supra* note 25.

50. *See* Krebs, *supra* note 25.

51. *See* Lewis, *supra* note 24, at 307 (discussing how “technology moves faster than the law” (quoting New York Times reporter Nick Bilton)).

52. *See* McCutcheon, *supra* note 1, at 221, 235–37, 240–41.

53. *See id.* at 225–26, 238. *See also generally* *About Defense Distributed*, DEF. DISTRIBUTED, <https://defdist.org/about/> [<https://perma.cc/5H48-V8JC>] (last visited Mar. 12, 2018).

54. *See* McCutcheon, *supra* note 1, at 226 (discussing Defense Distributed's mission to create a fully-printable gun).

55. *See id.* at 227.

56. *See* Cyrus Farivar, “Download this Gun”: 3D-Printed Semi-Automatic Fires Over 600 Rounds, *ARS TECHNICA* (Mar. 1, 2013, 6:00 AM), <https://arstechnica.com/tech-policy/2013/03/download-this-gun-3d-printed-semi-automatic-fires-over-600-rounds/> [<https://perma.cc/V5JG-2GN6>]; McCutcheon, *supra* note 1, at 227.

Homemaking 3D-printed guns is appealing because it allows for complete customization, and production is inexpensive and convenient.⁵⁷ Besides the 3D printer itself, the total cost to print a functioning firearm can be as low as three to ten dollars.⁵⁸ Furthermore, if made from plastic, they are easily disposable and may be melted down after use, exacerbating the current lack of serial numbers and other systems in place to track firearms.⁵⁹ For these reasons, 3D printing is especially attractive to hobbyists who may see self-creating a gun as a “technical challenge.”⁶⁰

The process has come a long way since its inception. The first 3D printers could not print all of the working parts of a gun, requiring gunsmiths to print individual parts and add those pieces to an already-existing firearm.⁶¹ Now, printing the gun itself is possible by simply filling a 3D printer with the chosen material and connecting it to a computer loaded with the desired design file.⁶² On GrabCAD.com alone, there are nearly 2,000 blueprints for guns and related parts.⁶³ Once the computer software processes the CAD file, the user initiates the printing process, and layer-by-layer, a functioning firearm is created.⁶⁴

However, firearms created with completely printed parts must overcome a significant challenge: achieving compatibility with traditional ammunition.⁶⁵ Originally, 3D-printed guns were typically made from plastic, and the heat and pressure generated by traditional ammunition caused parts of the gun to explode or crack.⁶⁶ Although one developer claimed to have shot fourteen rounds using traditional ammunition, most 3D-printed guns broke when taking their first shots.⁶⁷ However, a Pennsylvania man recently created a printable bullet that causes less wear on 3D-printed firearms.⁶⁸ Compared to traditional ammunition, the bullet has a thicker and longer shell, and the cartridge itself contains all the pressure generated by gunpowder upon pulling

57. See McCutcheon, *supra* note 1, at 226; CAMPBELL ET AL., *supra* note 44, at 5–7.

58. See Harlan, *supra* note 7, at 29.

59. See McCutcheon, *supra* note 1, at 236, 240.

60. See *id.* at 226.

61. See *id.*

62. See *id.* at 222–23.

63. See GRABCAD, https://grabcad.com/library?page=18&per_page=100&time=all_time&sort=recent&query=gun [<https://perma.cc/ZGA2-ANPB>] (last visited Mar. 29, 2017).

64. See McCutcheon, *supra* note 1, at 223.

65. See Lance Ulanoff, *Now There Are Bullets That Won't Break Your 3D-Printed Gun*, MASHABLE (Nov. 6, 2014), <http://mashable.com/2014/11/06/bullets-3d-printed-gun/> [<https://perma.cc/37QU-8URV>].

66. See *id.*

67. See *id.*

68. See *id.*; Harlan, *supra* note 7, at 28.

the trigger.⁶⁹ Federal law prevents him from selling the bullets without a license, but he plans to release the blueprints on his website so anyone can download and print the bullets.⁷⁰

Although bullets can be printed, gunpowder cannot.⁷¹ The chemical makeup of gunpowder, which creates the necessary explosive reaction, is beyond the capabilities of a 3D printer and is “scientifically very difficult” to replicate using such a device.⁷² However, gunpowder is easily obtained in sporting goods stores or online, and does not require that the buyer have any special license or registration to purchase it.⁷³

C. DEFENSE DISTRIBUTED AND THE FIRST 3D-PRINTED HANDGUN

In 2012, Cody Wilson and Ben Denio founded Defense Distributed, an “anti-monopolist digital publishing” corporation, with the mission of “defend[ing] the human and civil right to keep and bear arms . . . [and] to collaboratively produce, publish, and distribute to the public information and knowledge related to the digital manufacture of arms.”⁷⁴ The organization is an online platform that provides weapons blueprints to further its goal of reducing government and corporate interference with weapons manufacturing.⁷⁵ Wilson, in particular, is clear in his mission to provide widespread access to munitions.⁷⁶ In 2013, Defense Distributed announced

69. See Ulanoff, *supra* note 65.

70. See Harlan, *supra* note 7, at 28.

71. See Little, *supra* note 16, at 1508.

72. See *id.*

73. See Brendan J. Healey, *Plugging the Bullet Holes in U.S. Gun Law: An Ammunition-Based Proposal for Tightening Gun Control*, 32 J. MARSHALL L. REV. 1, 5–9 (1998). This article proposed regulating all ammunition, and ammunitions dealers themselves, under the Brady Handgun Violence Prevention Act as an all-encompassing solution for handgun violence in the United States. However, the article was written over a decade before 3D-printed guns were a reality. This Note builds on Healey’s proposal—an expanded Brady Bill—in a world where consumers now have the capability to manufacture weapons in their own homes through the use of a 3D printer. As discussed *infra*, 3D-printed guns lead to numerous gun control issues, such as having the capability to increase the number of illegally possessed guns. Because gunpowder cannot be printed, it is likely that the most readily available solution for remedying the issues posed by 3D-printed firearms is to regulate ammunition. See *infra* Part IV.

74. DEF. DISTRIBUTED, *supra* note 53; *DD History*, DEF. DISTRIBUTED, <https://defdist.org/dd-history/> [<https://perma.cc/GCW3-HKKH>] (last visited Mar. 12, 2018).

75. See Lewis, *supra* note 24, at 305 (noting that Defense Distributed identifies its mission as causing “disintermediation of state governments and large, collusive corporations”).

76. See Andy Greenberg, *Meet the ‘Liberator’: Test-Firing the World’s First Fully 3D-Printed Gun*, FORBES (May 5, 2013, 5:30 PM), <http://www.forbes.com/sites/andygreenberg/2013/05/05/meet-the-liberator-test-firing-the-worlds-first-fully-3d-printed-gun/> [<https://perma.cc/C59E-Q8ZR>] (discussing Wilson’s goal of “enabling individuals to create

that it had created the first functioning 3D-printed handgun, the “Liberator.”⁷⁷ In only four hours, Wilson printed fifteen of the sixteen parts necessary to create the gun.⁷⁸ He added a final piece, a metal firing pin, which can be purchased from a hardware store.⁷⁹

To create the Liberator, Wilson leased a printer from Stratasys,⁸⁰ a 3D-printing solutions company. When Stratasys discovered how Wilson planned to use the equipment, it seized the printer in fear of violating federal weapons laws.⁸¹ Unstoppable in his mission, Wilson acquired a secondhand Stratasys printer and, using ABS plastic, a heat-resistant material, printed the Liberator.⁸² The Liberator shoots standard .380 bullets and can fire several rounds.⁸³ Wilson immediately posted the Liberator’s blueprints online, making it the first “open-source weapon.”⁸⁴ Within two days of Wilson’s posting, the Liberator’s schematics were downloaded over 100,000 times.⁸⁵

The Liberator was the first major step toward proving that “anyone can print a gun in their bedroom.”⁸⁶ More recently, Defense Distributed released the “Ghost Gunner,” a CNC mill,⁸⁷ which provides hobbyists an alternative method for creating unregulated firearms.⁸⁸ On their website, Defense

their own sovereign space” and “demonstrat[ing] how technology can circumvent laws until governments simply become irrelevant”).

77. *See id.* This announcement immediately followed the Boston Marathon bombing, which involved homemade weapons.

78. *See* McCutcheon, *supra* note 1, at 227–28; Greenberg, *supra* note 76.

79. *See* Lewis, *supra* note 24, at 308; Greenberg, *supra* note 76.

80. *See* Lewis, *supra* note 24, at 305; STRATASYS, *supra* note 41.

81. STRATASYS, *supra* note 41.

82. *See* McCutcheon, *supra* note 1, at 227–28.

83. *Id.* at 228.

84. *See id.* The term “open source” was coined by the Open Source Initiative and applies to source code that is freely distributable. To qualify as “open source,” the Open Source Initiative requires that the code or software is freely distributable, includes source code, allows for modifications and derived works, has a readily available source, does not discriminate against any group or person, does not discriminate against fields of endeavor, includes redistributable licenses that are not product specific or restrictive of other software, and is technology neutral. For further explanation of “open source,” see *The Open Source Definition (Annotated)*, OPEN SOURCE INITIATIVE, <https://opensource.org/osd-annotated> [<https://perma.cc/5FFZ-257L>] (last visited Mar. 1, 2017).

85. *See* McCutcheon, *supra* note 1, at 245.

86. *See* Lewis, *supra* note 24, at 306.

87. Unlike a 3D printer, which uses an additive process, a CNC (computer-numerically-controlled) mill carves digital designs into the desired material using a drill. *See* Andy Greenberg, *The \$1,200 Machine That Lets Anyone Make a Metal Gun at Home*, WIRED (Oct. 1, 2014, 6:30 AM), www.wired.com/2014/10/cody-wilson-ghost-gunner/ [<https://perma.cc/2PQL-GWMG>].

88. *See* *Ghost Gunner 2*, DEF. DISTRIBUTED, <https://ghostgunner.net/> [<https://perma.cc/MW6D-KHZU>] (last visited Mar. 12, 2018) (“Due to Federal regulatory

Distributed advertises the Ghost Gunner saying, “With simple tools and point and click software [and] [n]o prior CNC knowledge or experience [you can] [l]egally manufacture unserialized AR rifles in the comfort and privacy of your home.”⁸⁹

Across the country, many legislators sprang into action following the unveiling of the Liberator and the Ghost Gunner.⁹⁰ Philadelphia became the first city to regulate the use of 3D printers, enacting an ordinance that requires one to have a federal manufacturing license to produce 3D-printed guns or their components.⁹¹ Although the ordinance was admittedly preemptive, Philadelphia’s policymakers found it more important to stay ahead of the quickly developing technology.⁹² The State Department acted similarly and sent Wilson a formal letter demanding he remove the Liberator’s blueprints from Defense Distributed’s website, claiming Wilson violated the International Traffic in Arms Regulations (“ITAR”),⁹³ which makes it unlawful to export technical data without authorization from the Directorate of Defense Trade Controls.⁹⁴

This was the first time in the State Department’s nearly forty years of regulating munitions “export[s]” that it sought enforcement against an Internet posting.⁹⁵ In response, Defense Distributed removed the blueprints and filed for authorization as required by the State Department.⁹⁶ However, the files continued to be shared across other websites.⁹⁷ Defense Distributed has since sought prior authorization before posting any new digital blueprints, but the State Department has yet to approve a single one.⁹⁸

overreach, Ghost Gunner is now the only affordable CNC solution for privately finishing your 80% lower receivers.”).

89. *Id.*

90. *See* Lewis, *supra* note 24, at 308.

91. *See id.* The ordinance stated, “No person shall use a three-dimensional printer to create any firearm, or any piece or part thereof, unless such person possesses a license to manufacture firearms under Federal law, 18 U.S.C. § 923(a).” PHILA., PA., CODE § 10-2002 (2018).

92. *See* Lewis, *supra* note 24, at 308 (discussing divergent views of proactively legislating 3D-printed weapons before printers are truly prevalent among individual consumers).

93. *See* Julia Cosans, *Between Firearm Regulation and Information Censorship: Analyzing First Amendment Concerns Facing the World’s First 3-D Printed Plastic Gun*, 22 AM. U. J. GENDER SOC. POLY & L. 915, 918 (2014).

94. *See* Def. Distributed v. U.S. Dep’t of State, 838 F.3d 451, 462 (2016) (Jones, J., dissenting).

95. *Id.*

96. *See id.* at 456.

97. *Id.*

98. *Id.*

D. *DEFENSE DISTRIBUTED V. U.S. DEPARTMENT OF STATE*

In the interim, Defense Distributed sued the State Department to enjoin it from enforcing ITAR.⁹⁹ Defense Distributed argued that the State Department's interpretation of the regulation constituted prior restraint on constitutionally protected speech.¹⁰⁰ Defense Distributed asserted a "hybrid claim," arguing the State Department violated both its First and Second Amendment rights.¹⁰¹ Additionally, Defense Distributed sought relief through a preliminary injunction to allow its files to remain online temporarily until the litigation's resolution.¹⁰² The district court denied the injunction, maintaining that Defense Distributed did not meet its burden of showing that its interest in protecting its constitutional rights outweighed national security concerns.¹⁰³ Defense Distributed appealed to the Fifth Circuit Court of Appeals.¹⁰⁴

The Fifth Circuit acknowledged that the act of privately printing firearms is lawful, but it narrowly focused its opinion on the legality of sharing firearms blueprints online that may be accessed by almost anyone worldwide.¹⁰⁵ The Fifth Circuit held that the district court did not abuse its discretion in denying the preliminary injunction, and remanded the case to the district court for further proceedings.¹⁰⁶ Judge Edith H. Jones dissented from the opinion, warning that the majority's affirmation will encourage the State Department to "threaten and harass" other individuals posting similar information online.¹⁰⁷

The procedural posture in the case limited the Fifth Circuit's ability to discuss the case's merits beyond the legitimacy of the preliminary injunction. However, the court recognized that on remand, the district court must address

99. *Id.*

100. *Id.*

101. *See id.*; Kyle Langvardt, *The Doctrinal Toll of "Information as Speech"*, 47 LOY. U. CHI. L.J. 761, 767 (2016).

102. *Def. Distributed*, 838 F.3d at 456.

103. *See id.* at 458. To be granted a preliminary injunction, the party must meet four requirements. The party must show:

(1) a substantial likelihood that he will prevail on the merits, (2) a substantial threat that he will suffer irreparable injury if the injunction is not granted, (3) that his threatened injury outweighs the threatened harm to the party whom he seeks to enjoin, and (4) that granting the preliminary injunction will not disserve the public interest. "We have cautioned repeatedly that a preliminary injunction is an extraordinary remedy which should not be granted unless the party seeking it has 'clearly carried the burden of persuasion' on all four requirements."

Id. at 456–57.

104. *Id.* at 453.

105. *See id.* at 455.

106. *Id.* at 460.

107. *See id.* at 462.

several issues, including (1) whether 3D-printing files are protected speech under the First Amendment, (2) the level of scrutiny applicable to the regulations, (3) whether posting files online to be freely downloaded constitutes “export,” and (4) whether ITAR’s regulatory scheme is unconstitutional prior restraint under the First Amendment.¹⁰⁸

III. STARING DOWN THE BARRELL: SCRUTINIZING 3D-PRINTED GUNS UNDER CURRENT LAW

The ability to self-manufacture weapons is protected under the law, and the current firearms regulatory scheme was written under this assumption.¹⁰⁹ Currently, very few individuals make their own firearms.¹¹⁰ Whereas self-manufacturing weapons has historically required specialized skills, 3D printing does not and therefore allows even novice gunsmiths to produce their own sophisticated weapons.¹¹¹ There are statutes currently in effect that may offer some control over 3D-printed guns, but they may need to be altered to provide adequate regulation.¹¹² By 3D printing guns, individuals have the capability to bypass federal regulations that dictate a firearm’s manufacturing, licensing, and registration requirements.¹¹³ Furthermore, any statute regulating 3D-printed firearms will likely be scrutinized under both the First and Second Amendments, requiring a balancing of public safety concerns with the constitutionally protected liberties of freedom of speech and the right to bear arms.¹¹⁴

A. THE CURRENT GUN CONTROL REGULATORY SCHEME AND ITS INABILITY TO REGULATE 3D-PRINTED FIREARMS

Federal, state, and local governments have taken numerous steps to control the prevalence of illegally possessed guns in the United States, with state and local governments enacting the majority of gun-related legislation because federal firearm legislation is limited.¹¹⁵ Although guns are heavily

108. *See id.* at 461.

109. *See* McCutcheon, *supra* note 1, at 239.

110. *United States — Gun Facts, Figures and the Law*, GUNPOLICY.ORG (Dec. 2, 2016), <http://www.gunpolicy.org/firearms/region/united-states> [http://perma.cc/96MV-KYCD].

111. *See* McCutcheon, *supra* note 1, at 239.

112. *See infra* Section 3.A.

113. *See id.*

114. *See infra* Section III.B.

115. McCutcheon, *supra* note 1, at 228. For a comprehensive list of state-enacted legislation, see Bindu Kalesan et al., *Firearm Legislation and Firearm Mortality in the USA: A Cross-Sectional, State-Level Study*, 387 LANCET 1847, 1849–50 (2016).

regulated, they are not truly “controlled.”¹¹⁶ There are hundreds of state and federal gun control statutes on the books,¹¹⁷ but because of gaps in federal legislation and conflicting state laws, the illegal gun market is flourishing.¹¹⁸ Furthermore, because individuals have not had an opportunity to self-produce guns as easily in the past, current firearm legislation is tailored towards acquiring and possessing commercially-made weapons.¹¹⁹ Thus, the ability to self-manufacture guns using a 3D printer complicates the already-complex issue of effective gun control regulation.

All states except Alaska and Vermont enforce some restrictions on concealed firearms.¹²⁰ However, state regulatory trends lean towards relaxed restrictions, opting for permit systems instead of total prohibitions on concealed carry.¹²¹ Similarly, the federal government currently enforces a licensing scheme, allowing most citizens to obtain firearms, with narrow exceptions for prohibited classes.¹²² Federal legislation includes: the Undetectable Firearms Act of 1988, the Arms Export Control Act of 1976, the Gun Control Act of 1968, the National Firearms Act of 1934, and the Brady Handgun Violence Prevention Act of 1993.¹²³ The Bureau of Alcohol, Tobacco, Firearms, and Explosives (the “ATF”) is charged with enforcing these statutes, issuing firearms regulations, providing federal firearm licenses,

116. See Little, *supra* note 16, at 1507.

117. See Susan Jones, *How Many Gun Laws Are There? Study Disputes 20,000 Number*, CNS NEWS (July 7, 2008, 8:20 PM), <http://www.cnsnews.com/news/article/how-many-gun-laws-are-there-study-disputes-20000-number> [<https://perma.cc/VCW7-64NL>]. Jones discusses a study by the Brookings Institution Center on Urban and Metropolitan Policy that found there are 300 “relevant” gun control statutes in the United States among federal and state governments, disputing a former report that there are 20,000 gun laws in the United States. *Id.* However, the study considered local laws “irrelevant.” *Id.*

118. See Daniel W. Webster, Jon S. Vernick, Emma E. McGinty & Ted Alcorn, *Preventing the Diversion of Guns to Criminals through Effective Firearm Sales Laws*, in REDUCING GUN VIOLENCE IN AMERICA: INFORMING POLICY WITH EVIDENCE AND ANALYSIS 109, 110–11 (Daniel W. Webster & Jon S. Vernick eds., 2013) (describing a study conducted by the ATF, which surveyed over 1,400 inmates with gun-related convictions, discovering that a mere 11.4% purchased their guns from a licensed dealer, with the majority of inmates stating that they stole their guns or purchased them through the black market).

119. See McCutcheon, *supra* note 1, at 240.

120. Philip J. Cook, Jens Ludwig & Adam M. Samaha, *Gun Control After Heller: Threats and Sideshows from a Social Welfare Perspective*, 56 UCLA L. REV. 1041, 1054 (2009).

121. *Id.*

122. See McCutcheon, *supra* note 1, at 228. Prohibited classes include felons, those with gun-related misdemeanors, drug and alcohol abusers, juvenile offenders, and the mentally ill. *Categories of Prohibited People*, LAW CTR. TO PREVENT GUN VIOLENCE, <http://smartgunlaws.org/gun-laws/policy-areas/background-checks/categories-of-prohibited-people/> [<https://perma.cc/RLJ4-DAX3>] (last visited Mar. 18, 2018).

123. 22 U.S.C. § 2778(a)(1) (2012); McCutcheon, *supra* note 1, at 229.

and conducting compliance inspections.¹²⁴ Currently, the ATF does not have much power over 3D-printed firearms and is only able to regulate them through gun control laws currently in place.¹²⁵

1. *The Undetectable Firearms Act of 1988*

The Undetectable Firearms Act of 1988 (“UFA”) makes it illegal to manufacture guns that cannot be detected by a metal detector.¹²⁶ The statute requires that all firearms contain at least 3.7 ounces of metal.¹²⁷ Additionally, the UFA requires that any firearm component, when viewed under an x-ray machine, maintain an accurate depiction of that component.¹²⁸ The UFA expired in 1998, but was extended for five additional years and then reauthorized for an additional ten years in both 2003 and 2013.¹²⁹

Criminals strive to go undetected and 3D-printed firearms, especially those made of plastic, can effectuate this goal. Currently, most printed guns are manufactured with some metal component, but as the technology progresses, this may change.¹³⁰ Even so, the metal presently used in printed guns, like the Liberator, is not substantial enough to set off any alarms.¹³¹ Recently, a group of Israeli journalists set out to test 3D-printed guns’ detectability, downloading and printing their own Liberator.¹³² Even with a metal firing pin in the gun, the journalists managed to go unnoticed through metal detectors, carrying the replicated Liberator into a meeting of the Israeli Parliament during the Prime Minister’s address.¹³³

Fully plastic firearms clearly violate the UFA. However, enforcement will be difficult because 3D-printed guns are becoming an inexpensive alternative to traditional firearms and can be produced in the privacy of one’s own home, where governmental oversight is functionally impossible.¹³⁴ Even if a printed firearm contains metal in compliance with the UFA, it may still go undetected,

124. See *Firearms*, ATF, <https://www.atf.gov/firearms> [https://perma.cc/TYW3-UV6P] (last visited Mar. 12, 2018).

125. See *What Say Does ATF Have in the Technology Used to Produce Firearms?*, ATF (Sept. 23, 2016), <https://www.atf.gov/firearms/qa/what-say-does-atf-have-technology-used-produce-firearms> [https://perma.cc/5ARH-QW2T].

126. See 18 U.S.C. § 922(p) (2012); Harlan, *supra* note 7, at 30.

127. § 922(p)(2)(C)(i).

128. See McCutcheon, *supra* note 1, at 226.

129. H.R. 3626, 113th Cong. (2013); McCutcheon, *supra* note 1, at 232.

130. See Harlan, *supra* note 7, at 30.

131. See Lewis, *supra* note 24, at 309.

132. See *id.*

133. See *id.*

134. See McCutcheon, *supra* note 1, at 226 (discussing the inexpensive aspects of the technology).

as in the case of the Israeli journalists.¹³⁵ Furthermore, some 3D-printed gun models have removable parts, so the owner could remove any metal while walking through a security detector and then put it back in place to fire the gun.¹³⁶

2. *Arms Export Control Act of 1976 and the International Traffic in Arms Regulation*

The Arms Export Control Act of 1976 (“AECA”) authorizes the President of the United States to control the import and export of “defense articles” and “defense services.”¹³⁷ It also grants the power to promulgate regulations for such imports and exports.¹³⁸ The President has the discretion to determine what constitutes defense articles and services, which are then added to the United States Munitions List.¹³⁹ The Munitions List does not list defense articles by name, but rather by specific attributes.¹⁴⁰ According to the regulations, “technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in [the Munitions List]” are considered defense articles.¹⁴¹ This includes information presented as blueprints, drawings, and instructions.¹⁴² The AECA imposes both civil and criminal penalties, with violations punishable by fines and imprisonment.¹⁴³

The AECA is enforced by the State Department.¹⁴⁴ The President has delegated the authority to make regulations under the AECA to the Secretary of State under ITAR.¹⁴⁵ ITAR requires authorization from the Directorate of Defense Trade Controls to “export” technical data related to any defense

135. See Lewis, *supra* note 24, at 309.

136. Rebecca Leber, *This Is the Only Gun Safety Bill That Passed Congress This Year*, THINKPROGRESS (Dec. 10, 2013, 1:45 PM), <https://thinkprogress.org/this-is-the-only-gun-safety-bill-that-passed-congress-this-year-f22ce0c0fd5b> [<https://perma.cc/T29D-J2VL>]. For these reasons, Congressman Steve Israel introduced the Undetectable Firearms Modernization Act of 2015 to better tailor the UFA to include 3D-printed weapons. H.R. 2699, 114th Cong. (2015); McCutcheon, *supra* note 1, at 232.

137. See 22 U.S.C. § 2778(a)(1) (2012).

138. See *id.*

139. See *id.*; *Def. Distributed v. U.S. Dep’t of State*, 838 F.3d 451, 455 (5th Cir. 2016).

140. See *Def. Distributed*, 838 F.3d at 455.

141. International Traffic in Arms Regulation, 22 C.F.R. § 120.6 (2018).

142. § 120.10(a)(1).

143. See § 2278(c) & (e). Violations are punishable by fines that may exceed one million dollars and prison terms of up to twenty years. *Def. Distributed*, 838 F.3d at 462 n.3 (Jones, J., dissenting) (citing 28 U.S.C. § 2778(c); *United States v. Covarrubias*, 94 F.3d 172 (5th Cir. 1996)).

144. See § 2778(i).

145. See *Def. Distributed*, 838 F.3d at 455.

article listed on the Munitions List.¹⁴⁶ Disclosing or transferring this data, including orally or visually, to a “foreign person” is considered an “export,” regardless of whether the transfer occurred in the United States or abroad.¹⁴⁷

In *Defense Distributed v. U.S. Department of State*, the State Department relied on ITAR, claiming that Defense Distributed’s published blueprints constituted technical data related to the Munitions List.¹⁴⁸ It claimed that posting these files online, which foreign nationals could access, equated to “export” and required prior approval from the State Department.¹⁴⁹ Courts have not yet determined whether posting gun-related digital blueprints online constitutes “export” under ITAR, a question intentionally left open by the Fifth Circuit in *Defense Distributed*.¹⁵⁰ If sharing digital weapons blueprints online is considered “export,” then the federal government may more strictly enforce the regulation to curtail the prevalence of 3D-printed firearms.¹⁵¹ However, this is unlikely, particularly as prepublication censorship is probably beyond the scope of ITAR.¹⁵²

Neither the AECA nor ITAR define the term “export.”¹⁵³ According to the dictionary cited by the Fifth Circuit, export is defined as “ship[ping] (commodities) to other countries or places for sale, exchange, etc.”¹⁵⁴ This definition implies the transmission of goods to foreign entities.¹⁵⁵ Based on this plain meaning, the term “export” does not include digital files that were uploaded domestically.¹⁵⁶ Furthermore, Congress presumably did not use vague statutory language, unintentionally deviating from the term’s plain

146. *See id.* at 463–64 (Jones, J., dissenting).

147. International Traffic in Arms Regulation, 22 C.F.R. § 120.17(a)(4) (2014); *see also Def. Distributed*, 838 F.3d at 462 (Jones, J., dissenting).

148. *Def. Distributed*, 838 F.3d at 456.

149. *Id.* at 455–56.

150. *See id.* at 461.

151. *See* International Traffic in Arms Regulation, 22 C.F.R. § 126 (2014).

152. *See Def. Distributed*, 838 F.3d at 466 (Jones, J., dissenting) (“Whether AECA itself, concerned with the ‘export’ of defense article related technical data, authorizes prepublication censorship of domestic publications on the Internet is at least doubtful.”).

153. *See id.*

154. *Id.* (quoting *United States v. Ehsan*, 163 F.3d 855, 858 (4th Cir. 1998)) (internal quotation marks omitted). The Fourth Circuit in *Ehsan* cited to “*The Random House Dictionary of the English Language* 682 (2d ed.1987).” *Ehsan*, 163 F.3d at 858.

155. *See Def. Distributed*, 838 F.3d at 467 (citing *Ehsan*, 163 F.3d at 858).

156. *See id.*

meaning.¹⁵⁷ Where a statute’s meaning is plain, a federal agency may not act beyond the scope of that meaning.¹⁵⁸

Additionally, it is doubtful that sharing digital weapons blueprints on a website, which may be accessed by anyone, will constitute “export” under ITAR.¹⁵⁹ Most online postings, particularly on websites such as the one at issue in *Defense Distributed*, are accessible to the public broadly.¹⁶⁰ These postings are distinguishable from past incidents of ITAR enforcement against defendants who, for example, tried to send WMD materials to North Korea, missile blueprints to China, or licensed chemical purchasing software to corporations owned by the Iranian government.¹⁶¹ Unlike these occurrences, where the shared information targeted a specific country or entity, posting CAD files to online platforms that are accessible to anyone does not have a direct, targeted contact. Overall, it is unlikely that posting digital firearms blueprints will constitute “export” under ITAR; and even if it were considered “export,” enforcement nonetheless may be blocked as unconstitutional under the First Amendment.¹⁶²

3. *The National Firearms Act of 1934, the Gun Control Act of 1968, and the Brady Handgun Prevention Act of 1993*

Congress enacted the National Firearms Act of 1934 (“NFA”) through its authority to tax, with an underlying goal of reducing the use of firearms in criminal endeavors, particularly by gangs.¹⁶³ It imposed a \$200 tax on the making and transfer of all enumerated firearms, including firearms and rifles with barrels less than eighteen inches long, machine guns, firearm mufflers, silencers, and “any other weapons.”¹⁶⁴ Although this tax was severe at the time of the statute’s enactment, the monetary amount remains the same today.¹⁶⁵

157. *See id.* (quoting *King v. Burwell*, 135 S. Ct. 2480, 2495 (2015)) (“Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions.”).

158. *See id.* (citing *Chevron U.S.A. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 842–43 (1984)).

159. *See id.* at 466 (describing how the government may prosecute individuals who directly email classified data to foreign persons or give them technical advice related to militant operations).

160. *See id.* at 462.

161. *See id.* at 465–66.

162. *See infra* Section III.B.1.

163. *See* National Firearms Act of 1934, 26 U.S.C. §§ 5801–72 (2012); *National Firearms Act*, ATF (Dec. 1, 2016), <https://www.atf.gov/rules-and-regulations/national-firearms-act> [<https://perma.cc/D8GJ-58XD>].

164. ATF, *supra* note 163.

165. *See id.*

The NFA also requires that the listed weapons be registered with the Secretary of the Treasury.¹⁶⁶ In the past, when individuals with unregistered NFA firearms attempted to register them, the Treasury could contact state authorities to report the unregistered weapon.¹⁶⁷ Practically, this became a Fifth Amendment self-incrimination issue and made the NFA unenforceable.¹⁶⁸ However, the Gun Control Act of 1968 (“GCA”) amended the NFA and remedied this defect.¹⁶⁹ Now, there is no mechanism for unregistered firearms already in one’s possession to be registered, and prosecutors are unable to use NFA registration applications against criminal defendants.¹⁷⁰

The GCA also imposes stricter gun control policies.¹⁷¹ Congress enacted the GCA in response to the assassinations of President John F. Kennedy, Attorney General Robert Kennedy, and Dr. Martin Luther King, Jr. to “provide support to Federal, State, and local law enforcement officials in their fight against crime and violence.”¹⁷² Through the GCA, Congress imposed stricter licensing requirements, established new firearm offenses, required firearms to bear a serial number, and banned sales to felons and other prohibited classes.¹⁷³ In particular, undocumented immigrants, illicit drug users, the mentally ill, felons, and those convicted of an act of domestic violence may not possess firearms under the GCA.¹⁷⁴ The statute further prohibits licensed dealers from selling firearms to those under the age of twenty-one, except in the case of rifles and shotguns, in which case the buyer must be eighteen.¹⁷⁵ Defendants with gun-related charges are most often prosecuted under the GCA’s provision that makes it “unlawful for a prohibited person to ship, transport, possess, or receive” a firearm.¹⁷⁶

In 1993, Congress amended the GCA by enacting the Brady Handgun Violence Prevention Act (the “Brady Bill”) to further limit prohibited classes

166. *Id.*

167. *Id.*

168. *See id.*

169. *See* Gun Control Act of 1968, 18 U.S.C. § 921 (2012); ATF, *supra* note 163.

170. *See* ATF, *supra* note 163.

171. *See* *Gun Control Act*, ATF (Sept. 22, 2016), <https://www.atf.gov/rules-and-regulations/gun-control-act> [<https://perma.cc/X2HS-GDP7>].

172. Gun Control Act of 1968, Pub. L. No. 90-618, § 101, 82 Stat. 1213; ATF, *supra* note 171.

173. *See* 18 U.S.C. § 921 (2012); ATF, *supra* note 171.

174. *See* 18 U.S.C. §§ 922(d)(1), (3), (4), (5)(A), (9) (2012).

175. *See id.* § 922(b)(1).

176. *See* McCutcheon, *supra* note 1, at 230.

from acquiring firearms.¹⁷⁷ The Brady Bill established the National Instant Criminal Background Check System (NICS) to be used by licensed firearms dealers before firearm transfers.¹⁷⁸ This system determines whether the purchaser is part of a prohibited class at the time of purchase.¹⁷⁹ The Brady Bill's requirements only apply to Federal Firearms Licensees, which include over 130,000 firearm manufacturers, dealers, and importers.¹⁸⁰ Since its enactment, the Brady Bill has prevented over two million prohibited persons from purchasing a firearm.¹⁸¹ However, there is a loophole for private sellers, who do not engage in the business of firearms dealing, to transfer guns without performing background checks.¹⁸²

It is uncertain whether 3D-printed guns are within the purview of the NFA, the GCA, and the Brady Bill at all.¹⁸³ The NFA may capture 3D-printed firearms if such firearms constitute “any other weapons” under the statute.¹⁸⁴ As defined, “any other weapons” includes “any weapon or device capable of being concealed on the person from which a shot can be discharged through the energy of an explosive.”¹⁸⁵ Nearly all 3D-printed guns will meet this definition, attaching the GCA's registration requirements and a \$200 tax upon their making.¹⁸⁶ However, since 3D-printed guns can be made at home, individuals who 3D print guns can easily evade these impositions, making it nearly impossible to enforce the GCA's licensing requirement.¹⁸⁷ Additionally, there is no way to control how an individual designs the printed gun, rendering the serial number requirement futile.¹⁸⁸

177. See H.R. REP. NO. 103-344, at 7 (1993) (“The purpose of [the Brady Bill] is to prevent convicted felons and other persons who are barred by law from purchasing guns from licensed gun dealers, manufacturers or importers.”).

178. See McCutcheon, *supra* note 1, at 231.

179. See *id.*

180. See 18 U.S.C. § 922 (2012); McCutcheon, *supra* note 1, at 231; *Fact Sheet – Federal Firearms and Explosives Licenses by Type*, ATF (Mar. 2016), <https://www.atf.gov/resource-center/fact-sheet/fact-sheet-federal-firearms-and-explosives-licenses-types> [<https://perma.cc/AQ3W-6A8C>].

181. *Effectiveness of the Brady Act and Background Checks*, LAW CTR. TO PREVENT GUN VIOLENCE, <http://smartgunlaws.org/effectiveness-brady-actbackground-checks/> [<https://perma.cc/VJV9-HSSX>] (last visited Mar. 13, 2018).

182. See McCutcheon, *supra* note 1, at 231.

183. See *id.* at 232.

184. See 26 U.S.C. § 5845(e) (2012).

185. *Id.*

186. See ATF, *supra* note 163.

187. See 18 U.S.C. § 923 (2012).

188. See Cook et al., *supra* note 120, at 1055 (noting current regulatory schemes are extremely difficult to implement).

Furthermore, self-manufactured 3D-printed guns clearly bypass mandated background checks under the Brady Bill. They are not purchased from a licensed dealer, but rather are most likely made in the privacy of one's own home. Prohibited persons, including felons, the mentally ill, and children and teenagers, can manufacture their own firearms, completely undermining the GCA's restrictions on prohibited classes.¹⁸⁹

B. CONSTITUTIONAL BARRIERS TO REGULATION: THE FIRST AND SECOND AMENDMENT

Printed firearms are controversial not only because of their dangerous nature but also because they likely implicate the first two amendments to the United States Constitution.¹⁹⁰ In its case against the State Department, *Defense Distributed* claimed it had an “extra-special First Amendment-Second Amendment ‘hybrid claim’ deserv[ing] even closer consideration.”¹⁹¹ *Defense Distributed* asserted that these two amendments together protect “expressive content about the right to keep and bear arms.”¹⁹²

1. *The First Amendment*

The First Amendment, sometimes referred to as “the First Freedom,”¹⁹³ guarantees one of the most fundamental rights—freedom of speech.¹⁹⁴ Textually, the First Amendment applies only to pure speech, as in spoken or written word.¹⁹⁵ However, the Supreme Court has held that the First Amendment protects more than literal speech, safeguarding freedom of expression through words, activities, and conduct.¹⁹⁶ Some have proposed a complete prohibition on sharing gun-related CAD files in order to block 3D printing illegal weapons at their source.¹⁹⁷ However, a growing body of scholarly work suggests that these digital blueprints likely constitute electronic speech subject to First Amendment protections.¹⁹⁸

189. See LAW CTR. TO PREVENT GUN VIOLENCE, *supra* note 122 (listing the GCA's prohibited classes).

190. See Blackman, *supra* note 13, at 504 (analyzing the “hybrid First and Second Amendments” and how they apply to 3D-printed guns).

191. Langvardt, *supra* note 101, at 767.

192. *Id.* at 767 n.15.

193. *Def. Distributed v. U.S. Dep't of State*, 838 F.3d 451, 476 (5th Cir. 2016) (Jones, J., dissenting).

194. U.S. CONST. amend. I.

195. Cosans, *supra* note 93, at 921.

196. *Id.* at 921–22.

197. See Blackman, *supra* note 13, at 499.

198. See *id.* at 501.

The *Defense Distributed* case illustrates the potential First Amendment concerns associated with prior restraint of CAD file publication. When Cody Wilson designed the Liberator, he uploaded its blueprints, consisting of CAD files, online.¹⁹⁹ Roughly 100,000 people downloaded the files within only three days of their posting.²⁰⁰ Because the CAD software requires specialized skills to operate, many individuals rely on online sources to access blueprints for what they seek to print.²⁰¹ There are numerous websites dedicated to offering users 3D-printable blueprints.²⁰² Accordingly, given the demand for this information and the expressive marketplace in which it occurs, scholars argue that this file sharing constitutes electronic speech, invoking First Amendment protection.²⁰³

In regulating speech under the First Amendment, there is a presumption that prior restraint is unconstitutional.²⁰⁴ Additionally, the degree of First Amendment protection for CAD files depends on the type of speech they are classified as.²⁰⁵ This characterization will dictate the level of scrutiny courts must apply in evaluating any future regulations.²⁰⁶ If CAD files constitute pure speech, or even expressive activity, laws controlling their distribution must satisfy strict scrutiny; such laws may also regulate the time, place, or manner in which the files are shared so long as the restrictions are content-neutral and leave open alternative channels for communication.²⁰⁷

Pure speech is given the highest level of First Amendment protection, prohibiting lawmakers from regulating the content of such speech unless such regulation passes the high bar of strict scrutiny.²⁰⁸ Conversely, if CAD files are considered expressive conduct, encompassing both speech and non-speech attributes, and they include elements of communication—in this case, the file

199. *Id.* at 485–86.

200. *Id.*

201. *See* McCutcheon, *supra* note 1, at 223.

202. *See, e.g.*, GRABCAD, *supra* note 37; THINGIVERSE, *supra* note 37.

203. *See, e.g.*, Blackman, *supra* note 13, at 499–502 (arguing that CAD files are electronic communications protected under the First Amendment); Cosans, *supra* note 93, at 930–36 (arguing that CAD files contain “sufficient” elements of communication to implicate the First Amendment).

204. *See* N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (recognizing the government’s heavy burden to justify limiting speech); *see also* Cosans, *supra* note 93, at 927 (noting that the government “bears a heavy burden of showing justification for prohibiting speech or expression”).

205. *See* Cosans, *supra* note 93, at 923.

206. *See id.*

207. *See id.* at 922; *see also* Def. Distributed v. U.S. Dep’t of State, 838 F.3d 451, 469 (5th Cir. 2016) (Jones, J., dissenting) (referring to the State Department’s actions as “pure content-based regulation”).

208. *See* Cosans, *supra* note 93, at 921.

sharing aspect—then burdensome regulations will be scrutinized under intermediate scrutiny.²⁰⁹ To be upheld under that standard, a regulation needs only to further a substantial government interest.²¹⁰

The Supreme Court has not yet spoken on how CAD files are classified under the First Amendment.²¹¹ However, lower courts continuously apply the First Amendment to computer code.²¹² Similarly, courts recognize that instructions, including blueprints, are protected speech.²¹³ Furthermore, the Supreme Court previously recognized that distributing photographs of guns, which are akin to gun-related digital drawings (i.e. CAD files), is constitutionally protected.²¹⁴ Therefore, CAD files, including gun-related blueprints, almost certainly qualify as speech, if not pure speech, and warrant First Amendment protection. Any regulation specifically targeted toward gun-related CAD files will likely be subject to heightened scrutiny, as such regulations would target a specific content-based subject and would not extend to all CAD files.²¹⁵

Furthermore, in *Defense Distributed*, the Fifth Circuit hinted that regulations regarding firearm-specific CAD files may qualify for strict scrutiny.²¹⁶ Although the majority focused on the injunction and reserved the merits for remand, the dissent offered an analysis of how 3D-printed firearms are protected under the First Amendment.²¹⁷ The dissent emphasized that if the government were able to regulate this kind of speech, regulations would likely encompass mediums beyond Internet postings.²¹⁸ The dissent criticized the majority for deciding the case on the basis of national security interests alone without even considering the broad-reaching effects that regulating content-

209. *See id.* at 923.

210. *See id.*

211. *See Def. Distributed*, 838 F.3d at 461; Cosans, *supra* note 93, at 921.

212. *See* Langvardt, *supra* note 101, at 768.

213. *See* Universal City Studios v. Corley, 273 F.3d 429, 451 (2d. Cir. 2001) (holding that computer code, and software programs made from that code, qualify as speech and are protected as such under the First Amendment).

214. *See* Brown v. Entm't Merchs. Ass'n, 564 U.S. 786, 804–05 (2011) (holding that violent video games, including those depicting gun violence, is protected speech under the First Amendment); Blackman, *supra* note 13, at 500–01.

215. *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 565–66 (2011) (noting that where a regulation imposes a “specific, content-based burden on protected expression . . . heightened judicial scrutiny is warranted”).

216. *See* Def. Distributed v. U.S. Dep't of State, 838 F.3d 451, 470 (5th Cir. 2016) (Jones, J., dissenting) (“Because the regulation of Defense Distributed’s speech is content-based, it is necessary to apply strict scrutiny.”).

217. *See id.* at 461–73.

218. *See id.* at 462.

based online speech may have on future cases.²¹⁹ By the time its case made it to the Fifth Circuit, Defense Distributed's ability to publish digital blueprints had already been hindered for three years.²²⁰ This was not a temporary injury, according to the dissent, but rather a trampling on Defense Distributed's First Amendment rights.²²¹

2. *The Second Amendment*

In addition to the First Amendment, any future regulation aimed at 3D-printed guns will be scrutinized under the Second Amendment.²²² The Second Amendment safeguards the right to "keep and bear Arms."²²³ Logically, this includes an implied right to acquire, and even self-manufacture, firearms.²²⁴ In 2008, the Second Amendment received its first substantive Supreme Court interpretation since the amendment was ratified over 200 years ago.²²⁵ In *District of Columbia v. Heller*, the Court held that gun ownership is an individual right, though not an unlimited one.²²⁶ In *Heller*, the Court struck down a Washington, D.C. handgun ban, focusing on the fact that handguns are widely used among the American people and potentially necessary for self-defense inside the home.²²⁷

The Court's holding in *Heller* protected the right to possess weapons "typically possessed by law-abiding citizens" in the home.²²⁸ Thus, under the Court's "in common use" test, firearms that are prevalent among the American people are protected under the Second Amendment.²²⁹ The Court stated that this test is "supported by the historical tradition of prohibiting the carrying of 'dangerous and unusual weapons,'" implicitly granting the ability to regulate

219. *See id.* at 461–63.

220. *See id.* at 463.

221. *See id.*

222. *See* Blackman, *supra* note 13, at 489–90.

223. U.S. CONST. amend. II.

224. *See* Blackman, *supra* note 13, at 491, 496; Little, *supra* note 16, at 1510–11.

225. Cook et al., *supra* note 120, at 1058. The pro-gun rights provision barely prevailed, passing with a 5-4 vote by the Court. *Id.* at 1059.

226. *See* *District of Columbia v. Heller*, 554 U.S. 570, 625–26 (2008); *see also* Cook et al., *supra* note 120, at 1059 (stating that the Court's opinion in *Heller* began "the process of accommodating an individualistic gun rights vision to the modern tradition of gun regulation").

227. *See Heller*, 554 U.S. at 628–29.

228. *See id.* at 625; Cook et al., *supra* note 120, at 1062.

229. *See Heller*, 554 U.S. at 624–28.

weapons that are “dangerous and unusual.”²³⁰ Therefore, it is likely that firearm ownership will be evaluated in light of the weapon’s popularity in the market.²³¹

In a 2017 case, *Kolbe v. O’Malley*, the United States District Court for the District of Maryland applied the “in common use” test to determine whether assault-style long guns can be lawfully possessed by private individuals.²³² That opinion provides insight into how lower courts may apply the “in common use” test to untraditional firearms.²³³ In determining the legality of the long gun, the Maryland court considered ownership statistics, the percentage of the total gunstock the weapon makes up, and whether the weapon is used for self-defense or another lawful purpose such as recreation.²³⁴ The Maryland court found that the long guns in question were likely dangerous and unusual.²³⁵ On appeal, the Fourth Circuit confirmed that these assault weapons were not protected under the Second Amendment.²³⁶

Under the reasoning in *Kolbe*, 3D-printed guns may not yet be considered “in common use,” in which case they would not be protected by the Second Amendment.²³⁷ Printed guns have only been in existence for four years as of this writing,²³⁸ and a significant portion of the population does not yet even own the technology to make them.²³⁹ Because 3D-printed guns are not in common use yet, it may be possible to regulate them under *Heller*’s “dangerous and unusual” exception.²⁴⁰ However, it is not necessarily the weapons themselves that are “unusual.”

230. *See id.* at 627.

231. *See id.* at 629 (discussing that handguns are one of the most popular self-defense weapons in America); *see also* Cook et al., *supra* note 120, at 1062 (stating that under *Heller*, handguns are viewed in light of their popularity, as opposed to machine guns, M-16s, and sawed-off shotguns, which the majority in *Heller* suggested would not be protected regardless of popularity).

232. *See* *Kolbe v. O’Malley*, 42 F. Supp. 3d 768, 788–89 (D. Md. 2014), *aff’d*, 849 F.3d 114 (4th Cir. 2017); Harlan, *supra* note 7, at 28.

233. *See* Harlan, *supra* note 7, at 28.

234. *See* *Kolbe*, 42 F. Supp. 3d at 784–90; Harlan, *supra* note 7, at 28.

235. *See* *Kolbe*, 42 F. Supp. 3d at 788. This court did not reach a final decision as to whether the ban on long guns violated the Second Amendment. *Id.* at 789.

236. *See* *Kolbe v. Hogan*, 849 F.3d 114, 121 (4th Cir. 2017). The Fourth Circuit avoided the question of whether the long guns were considered “dangerous and unusual,” basing its holding on the fact that these assault weapons are most useful in military service. *See id.* at 136–37.

237. *See* Harlan, *supra* note 7, at 31.

238. The first printed gun was made in 2013. *Id.*

239. *See id.*

240. *See id.* at 26.

Although some 3D-printed guns are readily distinguishable from the average store-bought gun, many are exact replicas of traditional firearms,²⁴¹ sharing nearly the same properties, such as their shape, firing power, and muzzle energy.²⁴² Thus, the main unusual—and potentially dangerous—aspect of 3D-printed guns is how they are manufactured. Unlike traditional firearms, which require specialized knowledge to make, 3D-printed guns may be created by completely inexperienced individuals.²⁴³ These individuals may be unfamiliar with the necessary materials and components of the weapon, or even unfamiliar with the operation of the firearm itself. Additionally, many users will likely rely on online CAD files whose sources may not be known or reliable, and whose designs may be flawed. Unfamiliarity with the materials, in addition to potentially flawed blueprints, could lead to catastrophic production safety issues, including guns that misfire or explode.²⁴⁴ These unique consumer safety issues may be able to bring 3D-printed firearms under the purview of the “dangerous and unusual” exception. However, since *Heller*, courts have not addressed whether weapons may be banned solely based on how they are produced.²⁴⁵ Therefore, it is possible that 3D-printed weapons may escape the “dangerous and unusual” exception and receive protection under the Second Amendment. Moreover, if and when 3D-printed guns become widespread,²⁴⁶ they will likely be considered “in common use,”²⁴⁷ particularly since the “in common use” test is not limited to weapons that existed at the time the Second Amendment was ratified.²⁴⁸

241. See McCutcheon, *supra* note 1, at 225–26.

242. See Jensen-Haxel, *supra* note 21, at 488–89.

243. See McCutcheon, *supra* note 1, at 239 (noting that although manufacturing a traditional gun requires “specialized knowledge,” “[t]oday, modern gunsmithing requires only a basic proficiency with computers and Internet access”).

244. See Liz Klimas, *Engineer: Don't Regulate 3D Printed Guns, Regulate Explosive Gun Powder Instead*, THEBLAZE (Feb. 19, 2013, 2:05 PM), <https://www.theblaze.com/news/2013/02/19/engineer-dont-regulate-3d-printed-guns-regulate-explosive-gun-powder-instead> [<https://perma.cc/VG2U-Y7XU>] (discussing one scholar's concern of the dangers that 3D printing firearms poses to hobbyists).

245. See Harlan, *supra* note 7, at 31.

246. It might be nearly impossible to determine at which point printed firearms become widespread. Unlike the long guns in *Kolbe*, it will be difficult to determine how many people actually own 3D-printed firearms, as there are no sales records, licenses, or serial numbers on which to rely. See *Kolbe v. O'Malley*, 42 F. Supp. 3d 768, 785–87 (D. Md. 2014); Harlan, *supra* note 7, at 31. One potential mechanism of establishing widespread use might be to analyze the number of times gun-related digital blueprints are downloaded; however, this seems unreliable as not every download is turned into a fully functioning firearm.

247. See Harlan, *supra* note 7, at 31.

248. See *District of Columbia v. Heller*, 554 U.S. 570, 582 (2008) (“Just as the First Amendment protects modern forms of communications . . . and the Fourth Amendment applies to modern forms of search . . . the Second Amendment extends, *prima facie*, to all

IV. TAKING AIM: ACHIEVING EFFECTIVE LEGISLATION

Printed firearms have the capability to evade federal gun control regulations almost completely.²⁴⁹ Because they can be created in the privacy of one's home, it is nearly impossible to enforce manufacturing, registration, or licensing requirements for such firearms.²⁵⁰ The technology also opens avenues for prohibited classes to print their own weapons, bypassing federally mandated background checks performed for traditional firearms purchases.²⁵¹ Furthermore, the First Amendment likely protects an individual's ability to share CAD files that can be used as blueprints for 3D-printed weapons, prohibiting the government from regulating these files without being subject to the strictest scrutiny.²⁵² Finally, following the Supreme Court's logic in *Heller*, 3D-printed guns are likely protected under the Second Amendment, which protects self-manufactured weapons and firearms that are in common use and not considered dangerous or unusual.²⁵³ In light of all of this, policymakers must tread carefully in attempting to regulate 3D-printed firearms.

A. THE CASE AGAINST REGULATING 3D PRINTING TECHNOLOGY

One possible approach to controlling the illegal possession and use of 3D-printed firearms is to regulate the 3D-printing technology itself. However, it is impractical to regulate any given aspect of 3D printing, as the technology by nature poses concrete challenges that are not easily isolated for effective regulation. Moreover, regulating the technology itself may also prematurely stifle its development, potentially resulting in greater detriment to society than the benefits that such regulation would bring.

As a practical matter, tracking who has 3D printers and what those individuals are printing would be difficult. One example of how the government could track the technology is to develop a system like the one used to uncover counterfeit printing.²⁵⁴ Companies, such as Hewlett-Packard, worked with the government to build a printing system that uses Printer Dots, which are microscopic yellow spots printed onto every document created by

instruments that constitute bearable arms, even those that were not in existence at the time of the founding.”).

249. See *supra* Section III.A.

250. See McCutcheon, *supra* note 1, at 221.

251. See Brady Handgun Violence Prevention Act, Pub. L. No. 103-159, 107 Stat. 1536 (1993) (codified at 18 U.S.C. §§ 921–922) (establishing criminal background checks for traditional firearm transfers).

252. See *supra* Section III.B.1.

253. See *Heller*, 554 U.S. at 624, 627–28.

254. See McCutcheon, *supra* note 1, at 241.

printers that are outfitted with that system.²⁵⁵ These spots provide the printer's serial number and make, so that law enforcement is able to track the document back to its particular printer, and presumably, to the person who printed it.²⁵⁶ However, to implement an effective system like the Printer Dots for 3D printing, manufacturers would need to develop a "spot" for every type of material that could be used in a 3D printer, which is highly impracticable given the abundance of different kinds of materials available for 3D printing.²⁵⁷

Alternatively, regulation could target 3D printing by prohibiting certain types of CAD files, such as firearm-related files. However, as discussed above, CAD files are likely protected under the First Amendment; therefore, any regulation of them must be narrowly tailored, or it will be struck down.²⁵⁸ Furthermore, online file sharing is nearly impossible to control. Although there are mechanisms used to police online postings, such as Content ID systems,²⁵⁹ users may find ways to evade these devices or use piracy websites to share prohibited CAD files.²⁶⁰ Additionally, tech-savvy individuals can manipulate the files to pass legal muster. For example, if firearm-related CAD files are prohibited, a designer could easily change the encryption of the file so that it would not resemble a gun, thereby avoiding restrictions.²⁶¹ Additionally, those skilled in CAD software will be able to altogether avoid regulations on publicly shared CAD files by simply creating their own digital blueprints.

Even if the government could practically regulate 3D-printing technology, doing so would likely stifle the benefits and possible advancements of 3D printing. In the past, the United States has been slow to regulate high-potential technology during the technology's infancy, in significant part because of the economic and social value of giving breathing room to young technological advancements. For example, when the Internet first began to experience widespread usage, the United States took a "hands off" approach to avoid inhibiting its potential.²⁶² In 1997, President Clinton issued an initiative

255. *See id.*

256. *See id.*

257. *See id.* at 241–42.

258. *See supra* Section III.B.1.

259. *See* Blackman, *supra* note 13, at 515.

260. *See* Stephanie Crawford, *How the Pirate Bay Works*, HOWSTUFFWORKS, <https://computer.howstuffworks.com/pirate-bay.htm> [https://perma.cc/3BPV-YHFM] (last visited Mar. 12, 2018).

261. *See* Blackman, *supra* note 13, at 516.

262. *See* Adam Thierer, *15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm*, FORBES (Feb. 12, 2012, 1:16 PM), www.forbes.com/sites/adamthierer/2012/02/12/15-years-on-president-clintons-5-principles-for-internet-policy-remain-the-perfect-paradigm/ [https://perma.cc/5X33-CJTZ] (discussing President Clinton's approaches to Internet policy in 1997).

consisting of “liberty-enhancing” principles to guide the Internet’s governance.²⁶³ His framework favored having the private sector lead the way through self-regulation, and was based on the idea that the Internet should develop in a market-driven arena with limited government involvement.²⁶⁴ He also noted that, due to the Internet’s novelty, regulatory schemes at that time might not have been well-suited for governance and might need to be revised or eliminated altogether.²⁶⁵

In regulating 3D printing, lawmakers must be careful not to inhibit beneficial technological growth,²⁶⁶ which arguably includes smarter weapons manufacturing. Given all the economic and social benefits 3D printing offers overall, it has the potential to overhaul how humans manufacture almost everything and could lead to the next great industrial revolution.²⁶⁷ In order to maximize the benefits of 3D printing, the technology should be broadly accessible so that it may be continually improved upon and advanced by innovators. Engineers, scientists, programmers, and even hobbyists need time to further develop 3D-printing technology in order to realize its full potential.²⁶⁸ Future regulations or bans concentrated on the technology itself may create additional costs, delays, or insurmountable roadblocks for inventors trying to improve the technology.²⁶⁹

Like its approach to the Internet, the United States should allow 3D-printing technology time to advance rather than risk stifling its innovation too greatly, too soon. Accordingly, the technology should be monitored for abuse, but legislative focus should remain on how to better control guns generally.²⁷⁰ The problems surrounding 3D-printed firearms, at least pertaining to their illegal possession and misuse, are best addressed through effective gun control broadly as opposed to regulating 3D-printing technology, CAD files, or 3D-printed firearms specifically.²⁷¹ Severely burdening the use of 3D-printing

263. *See id.*

264. *See id.*

265. *See id.*

266. *See* McCutcheon, *supra* note 1, at 246–47 (discussing the main objectives legislators should consider when regulating 3D-printing technology).

267. *See* Blackman, *supra* note 13, at 483.

268. *See* Jeremy Straub, *Does Regulating Artificial Intelligence Save Humanity or Just Stifle Innovation?*, QUALITY DIG. (Nov. 9, 2017, 1:03 PM), <https://www.qualitydigest.com/inside/innovation-column/does-regulating-artificial-intelligence-save-humanity-or-just-stifle> [<https://perma.cc/TH4J-4D5Z>] (discussing how regulation may stifle technological advancements in the context of artificial intelligence).

269. *See id.*

270. *See* Little, *supra* note 16, at 1509–10 (arguing it is better to find effective gun control measures than severely regulate technology).

271. *See id.*

technology is not only likely to infringe on constitutional rights but is also impractical and against the policy goal of protecting technological innovation, making it an inadequate method for curtailing illegal gun usage.²⁷²

B. REGULATING GUNPOWDER

Currently, the only regulated part of a firearm is its frame.²⁷³ The federal regulatory scheme relies on the ability to control the frame through serial numbers, licensing, and registration.²⁷⁴ Because 3D-printed weapons can be produced at home and therefore bypass all of those requirements, merely regulating a gun's frame will no longer be effective.²⁷⁵ To control the misuse of 3D-printed guns, lawmakers must look beyond the frame and concentrate on other available methods of gun control.

Now, and for the foreseeable future, 3D printers cannot create every single ingredient necessary to simply print, aim, and fire.²⁷⁶ Due to a necessary chemical reaction, printing gunpowder is not yet possible, and likely will be extremely difficult to accomplish.²⁷⁷ Modern ammunition has gunpowder built in, so individuals printing guns have two options for acquiring ammunition: either buy cartridges from local sporting goods stores or purchase gunpowder to insert into printed ammunition. Therefore, the most reasonable way to control 3D-printed firearms is to regulate ammunition. The simplest way to do this is to expand the Brady Bill to encompass ammunition purchases.²⁷⁸ Because most ammunition is pre-loaded with gunpowder, to regulate it effectively, it is necessary to extend the regulation to any purchase of ammunition containing gunpowder or a gunpowder alternative.²⁷⁹

An expanded Brady Bill would require all Federal Firearms Licensees to perform background checks on customers purchasing ammunition, which is defined in the Bill as “ammunition or cartridge cases, primers, bullets, or propellant powder designed for use in any firearm.”²⁸⁰ Alternatively,

272. *See id.* at 1510–11.

273. Jensen-Haxel, *supra* note 21, at 449.

274. *See id.* at 464.

275. *See id.* at 464–65.

276. *See* Little, *supra* note 16, at 1508 (noting that the “most significant limitation” on 3D printing a fully functioning firearm is creating the chemicals needed for an explosive reaction).

277. *See id.*

278. *See* Healey, *supra* note 73, at 3.

279. Bullets work through three main components: the primer, the propellant, and the bullet proper. The primer begins the chemical reaction. The propellant, which holds the gunpowder, is the chemical explosive. The bullet proper is the piece that actually hits the target. Chris Woodford, *Bullets and Missiles*, EXPLAINTHATSTUFF (Sept. 1, 2016), <http://www.explainthatstuff.com/bullets.html> [<https://perma.cc/BBE2-W9YY>].

280. 18 U.S.C. § 921 (2012).

purchasers may provide a qualifying Brady permit, which verifies that the purchaser is not a member of a prohibited class under the GCA and may legally buy ammunition.²⁸¹ Practically, amending the Brady Bill to include ammunition is relatively straightforward.²⁸² For example, the parts of the statute using the term “firearm” could be amended to say “firearm or ammunition.”²⁸³

According to a study performed at Boston University, expanding the Brady Bill to include background checks for the purchase of ammunition is the most effective form of gun control, in addition to background checks for firearm purchases.²⁸⁴ The study estimated that implementing background checks for ammunition purchases would decrease the firearm mortality risk by eighty-two percent.²⁸⁵ To strengthen this impact, the federal government should incentivize states to adopt similar legislation and expand background checks to all ammunition purchases.²⁸⁶

Heller implicitly approved the constitutionality of the current federal firearms regulatory scheme, which includes the Brady Bill. In particular, the Court stated:

[N]othing in our opinion should be taken to cast doubt on longstanding prohibitions on the possession of firearms by felons and the mentally ill, or laws forbidding the carrying of firearms in sensitive places such as schools and government buildings, or laws

281. Brady permits are an alternative to the Brady Bill’s background requirement and are valid for up to five years after issuance. The permit must be valid under the state’s law in which it is issued. For a comprehensive list of each state’s Brady alternative, see *Permanent Brady Permit Chart*, ATF (May 10, 2017), <https://www.atf.gov/rules-and-regulations/permanent-brady-permit-chart> [<https://perma.cc/X726-JLLM>].

282. See Healey, *supra* note 73, at 25–26.

283. See *id.* at 25.

284. See Kalesan et al., *supra* note 115, at 1847–54. The Boston University study analyzed the link between firearm legislation and firearm mortality by looking at state-specific firearm legislation. *Id.* It categorized each state by the type of legislation present in that state and then compared those categories to firearm mortality rates from each state, stratifying for intent (i.e., whether homicide or suicide). *Id.* It also accounted for unemployment, non-firearm homicides, firearm exports, and firearm ownership rates. *Id.* Overall, the study found nine laws that correlate to reduced firearms mortality, with the three strongest being universal background checks for firearms purchases, requiring firearm identification through microstamping or ballistics fingerprinting, and background checks for ammunition. *Id.*

285. *Id.* at 1853.

286. Three states—Illinois, Massachusetts, and New Jersey—currently require a Brady check for ammunition purchases. *Id.* at 1849. In 2015, Massachusetts had the lowest firearm mortality rate out of all fifty states. New Jersey was ranked sixth and Illinois ranked twelfth. *Firearm Mortality by State*, CTNS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/nchs/pressroom/sosmap/firearm_mortality/firearm.htm [<https://perma.cc/4RJH-7HUG>] (last visited Sept. 26, 2017).

imposing conditions and qualifications on the commercial sale of arms.²⁸⁷

It is therefore extremely likely that if the current federal regulatory scheme were expanded to enforce the same regulations over ammunition, it would be constitutional. By requiring background checks for ammunition purchases, prohibited classes could be effectively blocked from purchasing the necessary ingredients for homemade 3D-printed firearms. However, at the same time, legislators must be careful not to overly restrict access to ammunition.²⁸⁸ The Court has held that restricting the means to exercise an individual right is a violation of that right.²⁸⁹ In *Heller*, the Court solidified an individual's right to bear arms.²⁹⁰ *Heller's* holding would be moot if individuals were completely unable to access the ammunition necessary for firearms to function.²⁹¹

Although the Brady Bill has some loopholes,²⁹² its expansion would be a strong first step in curtailing the illegal possession and misuse of 3D-printed firearms while still safeguarding constitutionally protected rights. Gunpowder is the “unifying material everybody would need,” and without it, a 3D-printed gun would be inoperative.²⁹³ Expanding the Brady Bill to include background checks for ammunition purchases is the most readily available remedy to address the potential problems specifically posed by 3D-printed firearms. Amending the Brady Bill is relatively simple and less invasive for firearms dealers who already have access to the NICS used for firearms purchases. Of course, a black market may still exist for ammunition, and may even grow under an expanded Brady Bill.²⁹⁴ However, stricter regulations in the primary

287. *District of Columbia v. Heller*, 554 U.S. 570, 626–27 (2008).

288. *See* Blackman, *supra* note 13, at 513 (addressing constitutional limitations on regulating ammunition).

289. *See, e.g.*, *Minneapolis Star & Tribune Co. v. Minn. Comm’r of Revenue*, 460 U.S. 575, 591 (1983) (holding that taxing newspaper ink and paper violates the First Amendment’s freedom of the press); *see also* Blackman, *supra* note 13, at 513 (analogizing the tax in *Minneapolis Star & Tribune* to an all-out ban on gunpowder).

290. *Heller*, 554 U.S. at 591.

291. *See* Nicholas J. Johnson, *Administering the Second Amendment: Law, Politics, and Taxonomy*, 50 SANTA CLARA L. REV. 1263, 1265 (2010) (“Even though *Heller* did not explicitly address ammunition, it would eviscerate the right to say that guns are protected but ammunition is not.”).

292. *See* McCutcheon, *supra* note 1, at 231 (discussing the private seller loophole).

293. Robert Beckhusen, *3D Printing Pioneer Wants Government to Restrict Gunpowder, Not Printable Guns*, WIRED (Feb. 19, 2013, 6:30 AM), <https://www.wired.com/2013/02/gunpowder-regulation/> [<https://perma.cc/H2DC-VLZV>].

294. Healey, *supra* note 73, at 23. The state-level study included a cross-sectional analysis of gun control laws and their effect on firearm mortality in the United States. The most effective gun control laws in terms of lowering the firearm mortality rate were universal background checks for firearm purchases, background checks for ammunition, and requiring

market typically lead to higher prices in the secondary market.²⁹⁵ Price increases may act as an additional deterrent to those wanting to purchase ammunition illegally.²⁹⁶

V. CONCLUSION

Self-manufactured, 3D-printed guns present unprecedented legal challenges. The technology potentially enables anyone with a 3D printer to create fully functioning firearms in the privacy of the home, bypassing gun control laws.²⁹⁷ The current regulatory scheme cannot effectively control 3D-printed guns, which are likely protected under the First and Second Amendments.²⁹⁸ In enacting new regulations, it is vital that legislators strike the proper balance between public safety and civil liberties, while taking care not to block beneficial technological innovation. The best approach towards balancing those interests should focus on expanding the Brady Bill to impose safeguards on the purchase of ammunition. Regulating ammunition best comports with the long-standing provisions in federal firearm law broadly, the implicit holdings in *Heller*, and the technological challenges inherent in the advent of 3D-printing.

firearm identification through either microstamping or ballistic fingerprinting. When the results were adjusted to only include the law's effect on homicide rates, the law requiring background checks on ammunition was associated with the greatest reduction in firearm mortality rates. Kalesan, et al., *supra* note 115, at 1848, 1853.

295. See Healey, *supra* note 73, at 23–24.

296. See *id.*

297. See McCutcheon, *supra* note 1, at 221.

298. See *supra* Section III.B.

IP PRIVATEERING IN THE MARKETS FOR DESKTOP AND MOBILE OPERATING SYSTEMS

Daniel L. Rubinfeld[†]

ABSTRACT

Utilizing a privateering competitive strategy, firms sponsor the assertion of intellectual property (“IP”) claims by third parties (patent assertion entities and others), with the ultimate objective of raising of rival competitors’ costs. This Article tells the privateering story with respect to both desktop and mobile operating systems competition. It begins with Microsoft’s funding of litigation against Linux—a threat to Microsoft’s desktop operating system monopoly—and continues to an analysis of recent competition in the smartphone space. The Article raises potential competitive concerns and related antitrust and IP enforcement issues.

DOI: <https://doi.org/10.15779/Z38S46H60K>

© 2018 Daniel L. Rubinfeld.

[†] Robert L. Bridges Professor of Law and Professor of Economics Emeritus at U.C. Berkeley and Professor of Law at NYU. The author served as Deputy Assistant Attorney General for Economics during portions of the Clinton Administration. Aryan Jazayeri and Maxime Fisher-Zemin provided helpful research assistance. Participants in seminars at NYU and the University of Michigan as well as Robert Merges offered helpful comments.

TABLE OF CONTENTS

I.	INTRODUCTION	87
II.	EARLY PRIVATEERING	87
	A. THE LINUX THREAT.....	88
	B. THE GENESIS OF IP PRIVATEERING.....	90
	C. LESSONS FROM <i>SCO</i>	92
III.	THE GROWTH OF PRIVATEERING	94
	A. FUNDING A PRIVATEER: <i>SCO</i>	95
	B. CREATING A PRIVATEER: <i>NOKIA</i>	96
	C. TRANSFER FROM PAE TO PRIVATEER: <i>ROCKSTAR</i>	98
	D. TRANSFER FROM OPERATING COMPANY TO PRIVATEER: <i>MOSAID</i>	100
	E. SYSTEMATIZING PRIVATEERING: INTELLECTUAL VENTURES	101
IV.	PRIVATEERING IN THE SMARTPHONE OPERATING SYSTEM MARKET	102
	A. THE EMERGENCE OF SMART MOBILE DEVICES: <i>IOS</i> AND <i>ANDROID</i>	103
	B. EXTENSIONS OF THE <i>SCO</i> MODEL	108
	1. <i>Funding Third-Party IP Transfers: MOSAID</i>	108
	2. <i>Organizing Privateering Consortia: Rockstar</i>	110
	3. <i>Creating the Next SCO: Nokia</i>	112
	C. PRIVATEERING THROUGH INTERMEDIARIES: A ROLE FOR <i>IV?</i>	113
V.	PRIVATEERING CAN RAISE RIVALS' COSTS	114
	A. PATENT HOLD UPS	116
	B. ROYALTY STACKING	117
	C. PAES AS PRIVATEERS.....	119
	D. AN INNOVATION TAX	121
VI.	ANTITRUST IMPLICATIONS OF PRIVATEERING	123
	A. <i>NOERR-PENNINGTON</i> CONCERNS.....	124
	B. ATTRIBUTING ACTIONS OF PAE AGENTS TO THE PRIVATEERING SPONSOR.....	126
	C. SUBSTANTIVE ANTITRUST ISSUES.....	128
VII.	CONCLUSIONS	128

I. INTRODUCTION

Businesses in high-technology industries employ a variety of competitive strategies that depend on whether their goals are focused on short-run or long-run profitability, and whether their emphasis is on pricing or innovation. With the continued growth of the high-technology sector, a “new” competitive strategy has come to the fore: IP privateering. Under this privateering strategy, firms sponsor the assertion of IP claims by third parties (the so-called patent assertion entities (“PAEs”)), with the ultimate objective of raising rival competitors’ costs. Often, this privateering behavior is opaque to those being targeted.

How and why has IP privateering developed? When, if ever, is such behavior economically inefficient or anticompetitive? Should the potential for privateering be taken into account by competitive authorities when evaluating mergers and acquisitions (in the United States, under Section 7 of the Clayton Act)? Are there IP remedies that might reduce or eliminate the inefficiencies that flow from privateering? This Article discusses each of these questions in the context of a historical analysis of the two related markets—the markets for desktop and mobile operating systems.¹

The Article is organized as follows. Part II points to an early example of privateering—Microsoft’s funding of litigation against Linux, who represented a threat to Microsoft’s desktop operating system monopoly. Again using Microsoft as an illustration, Part III explains how the use of privateering grew over time as firms began to use third parties as intermediaries for pursuing intellectual property litigation that had the potential to raise rivals’ costs. Part IV brings the story up to the present by explaining how Nokia and a number of other IP entities have been transformed into privateers that are active in the smartphone industry. Part V describes potential competitive concerns that flow from privateering activities. Part VI completes the analysis by raising several antitrust and IP enforcement issues. Part VII offers several brief conclusions.

II. EARLY PRIVATEERING

In the mid-1990s, Microsoft learned what industrial organization economists would only come to appreciate fully some years later: for a dominant technology company, often the greatest risk to its entrenched

1. These markets are linked because the Android open-source operating system evolved in part from the Linux open-source desktop operating system. Steven J. Vaughan-Nichols, *Debunking Four Myths About Android, Google, and Open-Source*, ZDNET (Feb. 18, 2014, 10:54 PM), <http://www.zdnet.com/article/debunking-four-myths-about-android-google-and-open-source/> [https://perma.cc/M83Q-H2YT].

position comes, not from an entrant into its existing business, but from a disruptive technological or business-model change that facilitates the emergence of an entirely new product or way of doing business. As these disruptive products or services develop, they are initially likely to be partial substitutes for the existing product at best. However, over time, they may come to displace much if not most of the demand for that product or service.²

A. THE LINUX THREAT

In Microsoft's case, this disruptive threat initially came from the technological changes enabled by the rise of the Internet,³ particularly the development of Netscape's browser. In combination with Java (a cross-platform technology from Sun Microsystems), Netscape Navigator had the potential to reduce the most important entry barrier (the "applications barrier to entry") protecting Microsoft's Windows operating system monopoly.⁴

In early 1998, Netscape announced that it was publicly releasing the source code for its browser, and that future development would be done through the Mozilla Foundation, an open-source community.⁵ Netscape also indicated that Linux, a successful open-source operating system, would be a major operating system platform, thus promoting Linux as a rival to Windows.⁶ Not only did open-source's disruptive new business model make it a potential long-term desktop threat, it also posed a challenge to Microsoft in how best to competitively respond.

Microsoft's competitive response to the threat posed by Netscape and Java included conduct that ultimately led the Department of Justice (DOJ) to bring suit against the company for illegal monopolization in 1998.⁷ In findings

2. See Joseph L. Bower & Clayton M. Christensen, *Disruptive Technologies: Catching the Wave*, HARV. BUS. REV. (Jan.–Feb. 1995), <https://hbr.org/1995/01/disruptive-technologies-catching-the-wave> [<https://perma.cc/UM64-VAMY>].

3. For a discussion of Microsoft's view of the Internet threat, see Franklin M. Fisher & Daniel L. Rubinfeld, *U.S. v. Microsoft: An Economic Analysis*, 46 ANTITRUST BULL. 1, 19–23 (2001). For a recent overview of the legal issues raised in *United States v. Microsoft*, including an update on the state of Internet competition, see ANDREW I. GAVIL & HARRY FIRST, *THE MICROSOFT ANTITRUST CASES: COMPETITION POLICY FOR THE TWENTY-FIRST CENTURY*.

4. Fisher & Rubinfeld, *supra* note 3, at 20–21.

5. Janet Kornblum, *Netscape Sets Source Code Free*, CNET (Mar. 31, 1998, 12:10 PM), www.cnet.com/news/netscape-sets-source-code-free/ [<http://archive.is/5W34h>].

6. David Needle, *Why Intel and Netscape Bought Into Linux*, CNN (Oct. 1, 1998, 1:30 PM), <http://www.cnn.com/TECH/computing/9810/01/whylinux.idg/> [<https://perma.cc/CR8X-WUEN>].

7. Press Release, U.S. Dep't of Justice, Antitrust Div., Justice Department Files Antitrust Suit Against Microsoft For Unlawfully Monopolizing Computer Software Market (May 18, 1998), https://www.justice.gov/archive/atr/public/press_releases/1998/1764.htm [<https://perma.cc/67RD-3Q3P>].

affirmed on appeal, the DOJ showed that Microsoft had engaged in a variety of practices that were motivated by its effort to defend its dominant operating system monopoly.⁸ While the DOJ was successful in court on its core monopolization claims, Microsoft's efforts were no less successful in the marketplace. Indeed, by the early 2000s, Microsoft's browser share exceeded ninety percent,⁹ and Java has never been able to gain meaningful traction as a software application platform on "Desktop PCs."¹⁰

The disruptive threat from browsers and Java was not the last threat to its dominant desktop position that Microsoft faced. Only a few years later, Microsoft confronted a new threat, this time from a new business model: open-source software as evidenced by the Linux operating system. Linux represented a disruptive force because it enabled programmers—including applications programmers—to participate in the development of software through "virtual" communities outside existing firms. At the same time that Microsoft was defending its competitive strategy against Netscape and Java in court, it was becoming increasingly concerned that Linux was gaining traction in enterprise "servers" and might make the jump to the desktop as well.¹¹

It was in response to this new business model threat that Microsoft first began to use IP privateering as a competitive strategy.¹² Unlike most subsequent IP privateering, this involved the assertion of copyright rather than patent claims.¹³ In other respects, however, it involved many of the features that would later typify IP privateering by a variety of firms competing in the smartphone industry: funding the assertion of IP claims by third parties ("privateers"). The IP itself originated with a sponsor; the IP claims were targeted at downstream competitors of the sponsor (or their customers); and the connections between the sponsor and the privateering initiative were designed not to be transparent.¹⁴

8. *United States v. Microsoft Corp.*, 84 F. Supp. 2d 30, 46 (D.D.C. 1999), *aff'd in part*, 253 F.3d 34 (D.C. Cir. 2001).

9. *Id.* at 54; *see also Survey: Netscape Use Shrinks*, SILICON VALLEY BUS. J. (Aug. 28, 2002, 7:58 AM), <http://www.bizjournals.com/sanjose/stories/2002/08/26/daily30.html> [<https://perma.cc/46K3-S63F>] (noting that by 2002, Internet Explorer's global usage share reached ninety-six percent).

10. "Desktop" PCs include PCs that serve as "client" machines in a workplace client-server network.

11. Tom Ewing, *Indirect Exploitation of Intellectual Property Rights by Corporations and Investors*, 4 HASTINGS SCI. & TECH. L.J. 1, 55–56 (2012).

12. *See, e.g.*, David Balto, *Microsoft Makes an Empty Promise on Patents*, U.S. NEWS (Mar. 29, 2013, 3:25 PM), www.usnews.com/opinion/blogs/economic-intelligence/2013/03/29/time-for-transparency-on-microsofts-patent-troll-privateering [<http://archive.is/vUS05>].

13. *See, e.g.*, *SCO Grp., Inc. v. Novell, Inc.*, 721 F. Supp. 2d 1050 (D. Utah 2010).

14. Ewing, *supra* note 11, at 29 (noting some general characteristics of IP privateering).

In the remainder of this Section, I outline Microsoft's initial privateering effort through its funding of litigation by the SCO Group against Linux customers and distributors. Finally, I summarize some of the likely benefits as well as limitations from this initial privateering effort.

B. THE GENESIS OF IP PRIVATEERING

By 2001, open-source software had gone from a long-term threat for Microsoft to an immediate competitive concern.¹⁵ Also central to Microsoft's response to this competitive threat was promoting the intellectual property risk associated with Linux. Late in 2002, this led to Microsoft using an IP privateering strategy in connection with a copyright lawsuit filed in March 2003 by SCO Group against IBM, a prominent Linux developer and distributor.¹⁶ Unlike later IP privateering efforts, SCO already owned (or claimed to own—its ownership was later disputed) the IP that was the basis of the lawsuit.

In many respects, the *SCO* litigation shared a number of features that would become typical of later IP privateering. First, Microsoft's funding of SCO's activities was not readily apparent. Microsoft began with a sixteen-million-dollar payment in early 2003, far more than any license fees previously paid to SCO, which helped to validate the apparent strength of SCO's IP claim.¹⁷ At the same time, Microsoft secured an additional fifty million dollars for SCO indirectly, through an investment fund named BayStar Capital Management.¹⁸

A second feature of *SCO* that would become typical of later IP privateering was that the IP plaintiff, which had previously been an operating company, was in the process of becoming a litigation company. By having a nonpracticing entity like SCO litigate against IBM, Microsoft was able to effectively avoid the risk of countersuit that it would have faced if it had directly sued an IP-rich defendant like IBM.¹⁹ Notably, even after IBM obtained a declaration in 2006 attesting to Microsoft's funding of the litigation,

15. For a review of the rise of Linux and the open source movement, see generally Joel West & Jason Dedrick, *Open Source Standardization: The Rise of Linux in the Network Era*, 14 KNOWLEDGE TECH. & POL'Y 88 (2001).

16. Stephen Shankland, *SCO Sues Big Blue Over Unix, Linux*, CNET (Mar. 11, 2003, 8:34 AM), www.cnet.com/news/sco-sues-big-blue-over-unix-linux/ [https://perma.cc/ZND9-6J93].

17. Stephen Shankland, *Fact and Fiction in the Microsoft-SCO Relationship*, ZDNET (Nov. 15, 2004, 4:00 AM), <http://www.zdnet.com/article/fact-and-fiction-in-the-microsoft-sco-relationship/> [https://perma.cc/8LTT-4Z3B].

18. *Id.*

19. See Justin R. Orr, *Patent Aggregation: Models, Harms, and the Limited Role of Antitrust*, 28 BERKELEY TECH. L.J. 525, 535 (2013) ("Because NPEs do not practice any technology, they are practically invulnerable to the threat of patent counterclaims . . .").

IBM did not sue Microsoft—highlighting the practical limitations on the ability of a private defendant to take effective countermeasures against an IP privateering sponsor. Moreover, even against SCO, IBM's recourse was limited. IBM conclusively won the case on the merits, and SCO declared bankruptcy in 2007,²⁰ but IBM was still litigating collateral issues arising from the SCO litigation in 2013, *ten years* after the case was first filed.²¹

A third feature that *SCO* served to highlight was that IP privateering could be used to target a rival's potential customers. Creating a sense of direct financial risk on the part of potential Linux customers could be an effective competitive strategy. However, a direct approach creates a risk of backlash since customers could retaliate by switching to other vendors or simply delaying their purchases to punish the supplier. *SCO* demonstrated that IP privateering could be used successfully to solve this problem. In March 2004, a year after launching its litigation against IBM, *SCO* filed suit against two Linux customers: Daimler Chrysler and AutoZone.²² Virtually all of *SCO*'s funding for this litigation came directly or indirectly from Microsoft.²³

Fourth, and finally, *SCO* highlighted that an IP claim does not have to be strong on the merits to achieve its sponsor's competitive objectives. For example, in 2005, two years after the commencement of *SCO*'s suit against IBM, the district court observed that *SCO* had not offered credible evidence that IBM infringed *SCO*'s alleged copyrights through IBM's Linux activities.²⁴ Ultimately the court did not find that *SCO* owned the copyrights at issue, as Novell successfully sued for adjudication that it, not *SCO*, was the actual owner of the copyrights in question.²⁵

Despite these weaknesses in *SCO*'s case, it may nevertheless have been a successful competitive strategy. Indeed, Thomas Ewing has used the *SCO* litigation as an example of the effective use of IP privateering to increase IBM's cost of doing business and thereby slow its rate of adoption of a new business

20. Lee Hutchinson, *It's Back: District Court Judge Revives SCO v IBM*, ARS TECHNICA (June 17, 2013, 8:19 AM), <http://arstechnica.com/tech-policy/2013/06/its-back-district-court-judge-revives-sco-v-ibm/> [<https://perma.cc/VF4F-YTZZ>].

21. *Id.*

22. Stephen Shankland, *SCO Suits Target Two Big Linux Users*, CNET (Mar. 5, 2004, 5:46 AM), <http://www.cnet.com/news/sco-suits-target-two-big-linux-users/> [<https://perma.cc/5XMJ-PB8P>].

23. Shankland, *supra* note 17.

24. See Marius Meland, *Judge Denies Dismissal of SCO Copyright Suit vs. IBM*, LAW360 (Feb. 11, 2005, 12:00 AM), <http://www.law360.com/articles/3005/judge-denies-dismissal-of-sco-copyright-suit-vs-ibm> [<https://perma.cc/4RCA-79X3>]; Peter Fusco, *Wells Grans in Part IBM's Motion to Limit SCO's Claims! In *Large* Part*, GROKLAW (June 28, 2006, 5:52 PM) www.groklaw.net/article.php?story=20060628175203644 [[https://perma.cc/F2R\]-8S8B](https://perma.cc/F2R]-8S8B)].

25. *SCO Grp., Inc. v. Novell, Inc.*, 721 F. Supp. 2d 1050 (D. Utah 2010).

technology, noting that “the success of a privateering operation is the extent to which the sponsor (not the privateer) achieves its objectives.”²⁶

By the time the *SCO* litigation was dismissed, Microsoft had largely turned the corner on the competitive threat posed by Linux. Whether the IP privateering effort was a driving factor or not, to this day, despite Linux’s considerable success on servers and supercomputers,²⁷ its desktop presence remains minimal: as of March 2018, Linux’s desktop operating system market share was approximately 2.3%.²⁸

C. LESSONS FROM *SCO*

What lessons can a competitor draw from the *SCO* experience? First, IP privateering can be an effective competitive tool against a competitive rival. By targeting the rival’s customers, privateering can deter or slow the adoption rate of a new technology or business model.²⁹ In their article on strategic patent acquisitions, Fiona Scott Morton and Carl Shapiro provide an explanation for this outcome:

Younger products or businesses may have customers who are less attached to the product and have more elastic demand. The product may not be critical to the customer, but only desirable. A customer who is sued by a PAE over such a product may simply decide to stop buying the product.³⁰

This phenomenon may be even more pronounced with respect to prospective rather than actual buyers.

Second, the ability to target a rival’s customers through IP privateering can provide a solution to the challenge that arises when there is no single rival against which a company can focus its competitive efforts. IP privateering directed against downstream customers can enable a company to target a perceived weakness that is common to most if not all competitors. With respect to open-source, the perceived vulnerability was IP risk. The success of this tactic even with regard to an IP claim as weak as *SCO*’s (*SCO*’s Daimler Chrysler suit, for example, was summarily dismissed only four months after it

26. Ewing, *supra* note 11, at 57.

27. *About the Linux Foundation*, LINUX FOUND., <http://www.linuxfoundation.org/about/> [https://perma.cc/9S4C-VH6R] (last visited Mar. 10, 2018).

28. *See Desktop Operating System Market Share*, NETMARKETSHARE, www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0 [https://perma.cc/D6VK-LKJJ] (last visited Mar. 10, 2018).

29. *See* Fiona M. Scott Morton & Carl Shapiro, *Strategic Patent Acquisitions*, 79 ANTITRUST L.J. 463, 474 (2014).

30. *Id.*

was filed)³¹ highlighted an important competitive vulnerability that could be exploited through funding litigation against open-source customers.

Third, IP privateering appears to carry little antitrust risk. After defending against antitrust suits brought by DOJ with mixed results,³² Microsoft found that IP privateering could serve as a means of taking on emerging technology or business model threats with lower risk. The DOJ likely had some awareness of Microsoft's IP privateering; its inaction can reasonably be inferred to suggest that the privateering strategy was at a minimum less vulnerable than other challenged conduct.

Thus, while *SCO* had shown IP privateering to be a promising and effective new competitive strategy, the case also illustrated shortcomings associated with that strategy. For one thing, claims based in copyright rather than patent are hard to scale. Whereas patents can be readily bundled and sold, in packages of virtually any size, copyright claims cannot be so readily commoditized and marketed.³³ Patents, by comparison (particularly given the proliferation of software patents that had been issued by the PTO),³⁴ provide a far more promising option for engaging in IP privateering on a systematic and strategic basis.³⁵

31. Stephen Shankland, *SCO Flops in DaimlerChrysler Unix Lawsuit*, CNET (July 23, 2004, 4:16 PM), <http://www.cnet.com/news/sco-flops-in-daimlerchrysler-unix-lawsuit/> [https://perma.cc/47DV-8VWG].

32. *See* United States v. Microsoft Corp., 253 F.3d 34, 34 (D.C. Cir. 2001) (noting Microsoft's defense against the DOJ's claim that Microsoft had violated a 1995 antibundling consent decree was successful; however, the DOJ was largely successful in its 1999 monopoly maintenance case).

33. The low originality threshold of copyright law may pose another challenge for copyright claims; it allows putative infringers to relatively easily differentiate their software from copyrighted material. *See* Diana C. Obradovich, Garcia v. Google: *Authorship in Copyright*, 31 BERKELEY TECH. L.J. 785, 789 (2016) (explaining the low threshold imposed by the originality requirement).

34. *See* John R. Allison, Abe Dunn & Ronald J. Mann, *Software Patents, Incumbents, and Entry*, 85 TEX. L. REV. 1579, 1589–90 (2007) (explaining that entry is difficult when facing a patent thicket).

35. Another, probably less significant, difference between patents and copyrights is that patent claims are particularly difficult to resolve prior to extensive discovery and *Markman* hearings. *See, e.g.*, Peggy P. Ni, *Rethinking Finality in the PTAB Age*, 31 BERKELEY TECH. L.J. 557, 564 (2016) (noting that the high cost of patent litigation—even in nuisance suits by patent trolls—motivated Congress to create PTAB); Emily H. Chen, *Making Abusers Pay: Deterring Patent Litigation by Shifting Attorneys' Fees*, 28 BERKELEY TECH. L.J. 351, 357 (2013) (advocating for fee shifting provisions to deter frivolous patent lawsuits given the difficulty in resolving them early). Patents are therefore especially attractive from an IP privateering perspective, where claims only need to be “good enough” to get past Rule 11 and a motion to dismiss. (Indeed, for IP privateering purposes, patents that are “too good” might be relatively less attractive, as they are likely to cost more but provide little additional benefit to a privateering sponsor whose objective is unrelated to the merits of the litigation.)

For another thing, funding an IP privateering strategy through the use of intermediaries is unlikely to be effective without risk of public disclosure. Disclosure brings with it the possibility of countersuits by defendants and reputational harm with customers. Microsoft's use of a traditional investment fund, BayStar, in *SCO* was only moderately successful. BayStar's funding appears to have been based on more traditional investment metrics (such as an expectation of success on the merits), which ultimately led to substantial publicity with regard to Microsoft's role in *SCO*'s funding.³⁶

III. THE GROWTH OF PRIVATEERING

As IP privateering strategy evolved, companies shifted toward the assertion of patent rights over copyrights. Typically, there are three different types of parties involved: the operating company that developed the patents; the sponsoring company that seeks to use the patents for strategic purposes against downstream rivals; and the PAE that will be used to assert the patents against the downstream rivals. In some instances, however, where the operating company no longer has operating assets that can be targeted, the operating company itself can serve as the PAE.³⁷ Indeed, the operating company may also be the same as the sponsoring company, as in the case of Microsoft and Intellectual Ventures.

Just as there are three different types of entities that may be involved in a privateering effort, there are also three different ways in which the sponsoring firm might fund the privateering. In the simplest case, the PAE already controls the patents required for the privateering effort, and the sponsoring firm simply funds the targeting of enforcement efforts aimed at its downstream rivals. In other circumstances, the patents are still in the hands of the company that owns the related operating assets, and the sponsor funds the separation of the patents from the underlying assets in a way that results in the now-segregated patents in the hands of the PAE. On still other occasions, the patents already have been separated from the underlying operating assets, but they exist in a sufficiently large bundle that they can be disaggregated into smaller bundles to facilitate the imposition of higher costs on downstream rivals.

The subsections that follow describe the historical development of the privateering model: the funding of privateering (*SCO*), the creation of a new privateer (Nokia), the transition from a PAE to a privateer (Rockstar), the

36. Shankland, *supra* note 17.

37. In other cases, the parent might have a wholly-owned subsidiary handle any privateering functions. As a general rule, parent corporations are not liable for the acts of their subsidiaries. *See* United States v. Best Foods, 524 U.S. 51, 61 (1998).

transition from an operating company to a privateer (MOSAID), and finally the systemization of privateering (Intellectual Ventures).

A. FUNDING A PRIVATEER: SCO

PAEs' IP specialization and their relative immunity from countersuit put them in a strategic position that enables them to either impose substantial litigation costs or to utilize a threat to enter into profitable licensing arrangements.³⁸ The range of possible tactics include threatening the target company's entire business (for example, through threats of injunction or suits against customers); evading contractual or other commitments (such as the use of secrecy to evade existing licenses, or the refusal to abide by FRAND commitments³⁹); and imposing excessive damage awards (such as creating new PAEs so as to create royalty stacking, or making unreasonable royalty claims).⁴⁰ Where PAEs succeed in obtaining payments in excess of reasonable royalties, competition is harmed, both by causing downstream firms potentially to raise prices (thereby harming consumers), and by discouraging innovation if market participants are not being competitively compensated for their own research and development efforts.⁴¹

"Hybrid PAEs"—PAEs that have entered into a contractual relationship with a *downstream* firm to assert patents against that firm's rivals—pose an even greater competition risk. "Hybrid PAEs" are, in other words, privateers—PAEs that have been retained by a sponsor to target its downstream rivals with patent litigation and royalty claims. In addition to the usual effects of the strategy pursued by PAEs, there is an additional effect:

To the extent that the hybrid PAE successfully charges higher royalties for the patents it controls, it will raise the costs of the downstream firm's rivals. Facing rivals with higher costs, the downstream firm will benefit from incremental demand for its products. Additionally, outsized threats such as injunctions or customer lawsuits become less costly to carry out in this structure because they also drive demand away from rival products to the

38. Morton and Shapiro have observed that "devising outsized threats" of the pain to be inflicted on target companies from patent litigation "is a core competency of PAEs," and "[i]f the threat is large enough, and credible enough, the target firm will pay more than a reasonable royalty." Morton & Shapiro, *supra* note 29, at 472.

39. FRAND commitments are contractual commitments by standard-setting organizations to offer licenses at Fair, Reasonable, and Non-Discriminatory terms. See Benjamin C. Li, *The Global Convergence of FRAND Licensing Practices: Towards "Interoperable" Legal Standards*, 31 BERKELEY TECH. L.J. 429, 431–33 (2016) (describing FRAND agreements).

40. See Morton & Shapiro, *supra* note 29, at 472–78.

41. *Id.* at 483.

downstream firm's product where the downstream firm earns a margin.⁴²

Microsoft's arrangement with SCO appears to closely conform to a "hybrid PAE" model in which a PAE would approach a downstream firm with a proposal to "joint venture" against the downstream firm's rivals. In this example Microsoft is the sponsoring company to the patent assertion entity, SCO. It is plausible that SCO identified some of Microsoft's downstream rivals as possible litigation targets and then sought out Microsoft as a potential funding source for the litigation. Many of the tactics pursued by SCO, including the demand for outsized royalties, suits brought against customers, and secrecy surrounding Microsoft's sponsorship, are consistent with rational profit-maximizing economic behavior.

The competitive harm at the core of the "hybrid PAE" model—the combination of excessive royalties and rivals' increased costs likely to result from the combined efforts of a PAE and its downstream sponsor—can be found in subsequent privateering efforts by Microsoft. These subsequent efforts, however, are distinguishable from *SCO* in certain important respects. One is that, although the adverse *economic* consequences of the SCO arrangement may be discernible, as a *legal* matter the SCO-type arrangement may prove a significant challenge to antitrust litigation. Given that the patents are in the hands of the PAE at the time it approaches the downstream sponsor, the *Noerr-Pennington* doctrine may afford the downstream sponsor immunity from suit.⁴³

Furthermore, a "hybrid" PAE is likely to act opportunistically in finding sponsors interested in targeting particular downstream markets. A sponsoring firm committed to the use of privateering, by contrast, is likely to act systematically and with far greater cumulative impact on competition in the downstream market.

B. CREATING A PRIVATEER: NOKIA

Integral to the PAE business model is that the PAE does not operate in the downstream product market that is targeted by its patent enforcement efforts. By not participating in that market, the PAE can engage in the tactics that make outsized threats feasible, such as unreasonable demands, suits against customers, and disregard of implied or express contractual terms or reputational norms, while the PAE is protected by its functional invulnerability to countersuits or other tactics. In some instances, such as *SCO*, the company

42. *Id.* at 489–90.

43. Jeff McGoff, *Exploring the Boundary of the Noerr-Pennington Doctrine in the Adjudicative Process*, 34 U. MEM. L. REV. 429, 429–30 (2004) ("In the context of federal antitrust law, the Noerr-Pennington doctrine protects petition to the government . . . from antitrust liability.").

that owns the patents may have already exited (or begun to exit) the downstream market, and thus have turned itself into a PAE that can be used as a privateer.

Microsoft's arrangement with Nokia was different, in that Microsoft purchased the company's mobile operating assets, but left Nokia in possession of the related patent portfolio.⁴⁴ This raises the question: how should competition authorities analyze a transaction that *creates* the PAE privateer? Unlike SCO, Nokia still operated in the downstream market at the time of the transaction. Another part of the arrangement, therefore, involved Microsoft's purchase of Nokia's operating assets to enable it to operate as a PAE. This raises a further question: how should competition authorities analyze an acquisition in which ownership of the operating assets and related patents are segregated? Given the prevalence of excessive patents and the advantages that PAEs possess in terms of patent monetization, it is not difficult to envision that, in the future, it might be the case that the selling firm would find that its patent portfolio has greater value to a PAE (whether a third party or the selling firm as a new *de facto* PAE) than the patents do to the acquirer of its operational assets. Where the patents can be used to target rivals of the purchaser of the operational assets, it is likely to be even more profitable for the patents to be retained by the PAE, with the additional gains resulting from the patents' use in privateering divided between the PAE and the asset purchaser.

For purposes of analysis under the Clayton Act, although the segregated sale of the operational and patent assets might maximize the seller's return, it is not at all clear that competition authorities should view this outcome as reflecting a welfare-enhancing allocation of resources. This concern would exist even in the absence of privateering. It remains the case that a PAE's superior ability to monetize is more likely to reflect a tax on downstream firms that harms consumers in the short-run and innovation in the long-run, than an efficiency-enhancing arrangement. Of even greater concern, however, should be the segregation of ownership of the operational assets and patents where, as may often be the case, the patents can be targeted at competitors in the market in which the asset purchaser competes, and rivals of the asset purchaser do not have licenses to the patent portfolio.

Under those circumstances, it seems likely that a patent privateering arrangement is embedded in the sales transaction. Ironically, competition would probably be less adversely impacted if the asset purchaser also acquired

44. Dan Levine, *Why Nokia Didn't Sell Its Patents to Microsoft*, REUTERS (Sept. 3, 2013, 12:46 PM), www.reuters.com/article/us-nokia-microsoft-patents-idUSBRE9820ZZ20130903 [<https://perma.cc/9TLE-QFAS>].

the associated patents. Suppose, for example, that Microsoft had acquired not just Nokia's mobile assets but also its mobile patents. This would lessen the potential concerns of the competition authorities. The reason is that if the patents were in Microsoft's hands, downstream rivals or their customers would have had many counterstrategies available, for all the reasons downstream firms find it harder to monetize than PAEs: the possibility that the patents would fall within existing licenses, greater reputational harm from suing customers, greater vulnerability to countersuits, and so on. By "selling" the patents to Nokia in its new role as PAE, Microsoft could raise its rivals' costs much more effectively than if it had acquired the patents itself.

C. TRANSFER FROM PAE TO PRIVATEER: ROCKSTAR

The Nortel patents provided bidding entities with an opportunity to acquire a substantial patent portfolio disassociated from the underlying related operational assets. After the announcement of the Microsoft/Nokia strategic partnership, Nortel Networks, a telecommunications operating company with a substantial patent portfolio, put up for auction more than 4,000 patents related to wireless and Internet technologies.⁴⁵ Nortel had filed for bankruptcy in 2009, and the patents were amongst the final assets remaining to be sold in the bankruptcy court.

The \$4.5 billion winning bid in the Nortel auction—an amount several times larger than the patents had been expected to sell for before the auction commenced—was submitted by a consortium consisting of Microsoft and five other companies, through an entity named Rockstar Bidco (later renamed the Rockstar Consortium, Inc.).⁴⁶ Two of the other Rockstar participants—Apple and EMC—previously had joined Microsoft in another consortium (CPTN).⁴⁷

By the time it sold its patents in the bankruptcy auction, Nortel had disposed of its operational assets,⁴⁸ and therefore the company conceivably could have chosen to monetize its patent portfolio as a "pure" PAE. Nortel's

45. Alastair Sharp & Nadia Damouni, *Final Bids Due for Nortel Patents*, REUTERS (Dec. 9, 2010, 1:33 PM), <http://www.reuters.com/article/us-nortel-idUSTRE6B84FO20101209> [<https://perma.cc/9TLE-QFAS>].

46. See Dylan Bushell-Embling, *Courts Clear Rockstar JV to Buy Nortel Patents*, TELECOM ASIA (July 12, 2011), <http://www.telecomasia.net/content/courts-clear-rockstar-jv-buy-nortel-patents> [<https://perma.cc/PVS6-NYM6>].

47. See Press Release, U.S. Dep't of Justice, CPTN Holdings LLC and Novell Inc. Change Deal in Order to Address Department of Justice's Open Source Concerns (Apr. 20, 2011), <https://www.justice.gov/opa/pr/cptn-holdings-llc-and-novell-inc-change-deal-order-address-department-justices-open-source> [<https://perma.cc/R7DR-G5QR>].

48. Sean Michael Kerner, *Nortel's Last Gasp*, ENTERPRISE NETWORKING PLANET (Aug. 10, 2012), <http://www.enterprisenetworkingplanet.com/netsysm/nortels-last-gasp.html> [<https://perma.cc/FVR5-K85K>].

finding that it was more profitable to sell to Rockstar, a PAE organized by Android's downstream rivals and an obvious privateer, reflects the fact that it is likely to be more profitable to use patents for privateering than solely for generating royalties (even outsized ones, as a pure PAE might be expected to earn).⁴⁹

It is notable to compare the Rockstar transaction to an earlier sale of Novell patents to a consortium consisting of Apple, Oracle, EMC, and Microsoft. In the earlier Novell transaction, the patents were to be divided among these four downstream operating companies.⁵⁰ The Department of Justice appears to have challenged (with the threat of a lawsuit) Microsoft's acquisition of this portion of the Novell portfolio on vertical foreclosure grounds—namely, that the patents might have been an essential input for downstream Linux providers, and Microsoft would have had an incentive to withhold access to this input to these downstream rivals. Through an agreement with DOJ, Microsoft was forced to sell the patents back to the seller, and was only permitted only to retain a license to the patents.⁵¹

It is possible that the DOJ viewed Novell's patents as potentially blocking in a way that Nortel's were not, but the differential in the price of the two patent portfolios makes that seem unlikely: the Novell patents sold for \$450 million, while the Nortel patents sold for ten times that amount—\$4.5 billion. The final remaining difference is that the Novell transaction involved Microsoft's outright acquisition of the patents, while the Nortel patents were transferred to a PAE in which Microsoft was a part owner.

As discussed in Part II, the transfer of the patents to a privateering PAE can create a competition problem. While the direct acquisition of the Novell patents might seem problematic, downstream rivals had potential defenses they could bring to bear if Microsoft were to sue on these patents: the patents might have been covered by existing licenses or cross-licenses; Microsoft might have had a more difficult time suing customers who were also its own commercial customers or partners; Microsoft would have suffered substantial reputational damage from renegeing on the open-source commitments that Novell had made; and so on. Rockstar, by comparison, could engage in all of the tactics used by PAEs (threats of injunction, unreasonable royalty demands, and the like) to raise the costs of its owners' rivals, all the while enabling its

49. To be fair, one might view the payments for the Nortel patents, at last in part, as appropriate compensation for past technological contributions. For a more positive view of the role of patent trolls, see generally Michael Risch, *Patent Troll Myths*, 42 SETON HALL L. REV. 458 (2012).

50. Press Release, *supra* note 47.

51. *Id.*

owners to avoid the reputational and other costs that they might otherwise suffer.

D. TRANSFER FROM OPERATING COMPANY TO PRIVATEER: MOSAID

As a policy matter, the aggregation of patent rights can be more of a problem than the disaggregation of those rights, especially when those rights are sold to others. Disaggregation makes sense for “pure” PAEs because damage awards are likely to be increased if patent assertions are made by a variety of different firms. According to Lemley and Melamed:

Because patent damages are likely to include more than the incremental value of the patented technology itself, i.e., to include some product value not properly attributed to the asserted patent, the patent holder is more likely to be able to ‘double dip’ into that excess value by multiple assertions than if it asserts all its patents in a single case.⁵²

Nokia, spinning off thousands of patents to MOSAID, an intellectual property company that focuses on the licensing and development of semiconductor and communications technologies, provides one example. Lemley and Melamed note that, even where the operating company does not directly control the PAE, it is likely that it “is able as a practical matter to control or constrain the incentives of the troll. It might do so by contract or by selling patents that are already licensed to all but a few users of the patented technologies and thus directing the troll’s attention to the seller’s targets.”⁵³

While Nokia’s transfer of patents to MOSAID is representative of the potential problem raised by operating companies spinning off their patents to PAEs, the Nokia transaction did not simply involve an operating company unilaterally deciding to spin off some part of its assets to a PAE. This is significant inasmuch as there could be circumstances where an operating company decides to spin off some parts of its patent portfolios for reasons unrelated to privateering. For example, if part of an operating company’s portfolio reads on downstream markets other than the one in which it competes, it might determine that the patents can better be monetized by a PAE than by the operating company itself. Although this monetization effort might not be optimal for purposes of maximizing consumer welfare, it is not any more problematic from a competition perspective than any other entity (say, a university) spinning off its patents for monetization by a “pure” PAE.

52. Mark A. Lemley & A. Douglas Melamed, *Missing the Forest for the Trolls*, 113 COLUM. L. REV. 2117, 2159 (2013).

53. *Id.* at 2161.

The funding of MOSAID had the effect of raising the costs for downstream rivals. Moreover, whereas an operating company spinning off its own patents faces limits with respect to how many bundles its portfolio can be divided into (to create a stacking problem, each PAE must receive a sub-portfolio large enough and strong enough to credibly threaten to take a case to court),⁵⁴ there are effectively no natural limits on how frequently a company could fund the spinoff of some of another firm's patents for privateering use by a PAE.

It is undoubtedly the case that many firms in the information technology industry do not want to assert their patents, and other firms may fund privateering at one point in time but opt to avoid privateering at other times. However, there is little doubt that funding MOSAID-like transfers has the potential to be a “win-win-win” for the firms involved: a win for the operating company, by monetizing a part of its portfolio without having to litigate (which could jeopardize its business reputation or relationships); a win for PAE, by getting a portion of the returns it can earn from outsized demands; and a win for the privateering sponsor, by raising its rivals' costs while potentially even earning some returns from the PAE's efforts.

E. SYSTEMATIZING PRIVATEERING: INTELLECTUAL VENTURES

Intellectual Ventures (“IV”) was founded in 2000 by two senior Microsoft executives, Nathan Myhrvold (the company's chief technology officer) and Edward Jung (its chief architect).⁵⁵ Since IV was founded, Microsoft heavily invested in IV. Some part of this investment was in the form of financial backing: in 2006, for example, in the middle of the *SCO* litigation, Microsoft acknowledged a \$76 million investment in IV and an option for an additional \$40 million subsequent investment.⁵⁶ At its initial stage, IV was estimated to have 3,000 to 5,000 patents.⁵⁷

This systematic accumulation of patents by former Microsoft executives on behalf of IV would seem to raise substantial corporate opportunity questions if Microsoft were not benefiting substantially from IV's activities. The question then becomes what form this benefit might take. One possible

54. Morton & Shapiro, *supra* note 29, at 478.

55. See Tom Ewing & Robin Feldman, *The Giants Among Us*, 2012 STAN. TECH. L. REV. 1, 3 (2012).

56. Nicholas Varchaver, *Who's Afraid of Nathan Myhrvold?*, FORTUNE (June 26, 2006), http://archive.fortune.com/magazines/fortune/fortune_archive/2006/07/10/8380798/index.htm [<https://perma.cc/K4CE-JVYD>].

57. *Id.*

benefit to Microsoft would be if IV could serve as a reliable intermediary for the company in funding and managing privateering operations.

IV's highly secretive organizational structure and novel business model have been well suited with respect to privateering. It is notable that authors Robin Feldman and Thomas Ewing, with great difficulty, "pieced together 1276 shell companies associated with Intellectual Ventures," and, even then, admitted that "[w]e do not believe that we have identified all of the Intellectual Ventures shell companies"⁵⁸ As a result of this opaque structure, IV often was able to bring patent cases through intermediaries:

Until recently, Intellectual Ventures used third parties to carry out much of its litigation activities. . . . While we do not know the deal terms, we did, however, find many examples of Intellectual Ventures using third-party proxies to litigate infringement claims against companies who appear to be likely licensing targets for large portions of Intellectual Ventures' portfolio. In particular, many of the patents sold by Intellectual Ventures have ended up in litigations brought by their new acquirers.⁵⁹

IV was not only better suited to serve as a privateering intermediary than a conventional investment firm, but it was also better able to operate at the scale potentially required to make privateering successful. Prior to IV, PAEs consisted of individuals or small firms that typically owned fewer than 100 patents, and largely funded their acquisition and litigation activities through contingency legal arrangements. IV, by contrast, was able to begin to acquire patents by the thousands.⁶⁰ Scale not only creates efficiencies, it has a strategic competitive advantage. With scale, patent aggregators such as IV are relatively immune from patent-specific defenses; it is simply too costly to litigate the patent quality of thousands of patents.⁶¹

IV. PRIVATEERING IN THE SMARTPHONE OPERATING SYSTEM MARKET

Privateering has continued to be a useful competitive strategy as technology has moved us from a desktop-computing world to the world of smartphones, iPads, Kindles, and related devices. This Part begins with a characterization of the worldwide competition between the Apple and

58. Ewing & Feldman, *supra* note 55, at 4.

59. *Id.* at 13.

60. *Id.* at 5, 7–9.

61. Indeed, a survey by the American Intellectual Property Law Association found that, in 2013, the median litigation cost for a patent valued between \$1 and \$25 million was \$2.6 million. Patents valued over \$25 million had a median litigation cost of \$5.5 million. AM. INTELLECTUAL PROP. LAW ASS'N, REPORT OF THE ECONOMIC SURVEY 2013 at 34 (2013).

Android smartphone operating systems. The Sections that follow point out how the Nokia acquisition and the Rockstar and MOSAID transactions have, at times, been utilized for privateering purposes.

A. THE EMERGENCE OF SMART MOBILE DEVICES: IOS AND ANDROID

A revolution in modern telephony emerged from the opposite direction than the Linux threat in the early 2000s: instead of coming from operating systems optimized for more powerful devices (servers) located mostly in the enterprise, this time the modern telephony evolution came from operating systems optimized for less powerful devices (mobile phones) located mostly in the consumer space. Prior to 2007, mobile phones had extremely limited browser and other functionalities.⁶² Apple's mid-2007 introduction of the iPhone, however, followed the next year by the introduction of the first device based on the Android operating system (a Linux-based operating system Google had acquired in 2005), marked the beginning of a fundamental change in the capabilities of these devices.⁶³

When first introduced, Apple's smartphone was, as one reviewer summarized at the time, "the first smart phone we've tested with a real, computer-grade Web browser, a version of Apple's Safari. It displays entire Web pages, in their real layouts, and allows you to zoom in quickly by either tapping or pinching with your finger."⁶⁴ Prior to the iPhone, web browsers on mobile devices on smartphones had extremely limited capability, and therefore were used principally for dedicated applications such as email. Apple's smart phone, by contrast, enabled users to access the wide array of information available on the Internet. As one reviewer summarized, it represented "the evolution of the humble cellphone into a true handheld computer, a device able to replicate many of the key functions of a laptop."⁶⁵

User adoption of this new functionality was immediate and dramatic: six months after the iPhone's introduction, a news article reported that Google "said it has seen 50 times more search requests coming from Apple iPhones than any other mobile handset—a revelation so astonishing that the company

62. See Fred Vogelstein, *The Day Google Had to "Start Over" on Android*, ATLANTIC (Dec. 18, 2013), <http://www.theatlantic.com/technology/archive/2013/12/the-day-google-had-to-start-over-on-android/282479/> [<https://perma.cc/FR4X-RE8D>].

63. See *id.*

64. *The iPhone is a Breakthrough Handheld Computer*, ALL THINGS DIGITAL (June 26, 2007, 6:15 PM), <http://allthingsd.com/20070626/the-iphone-is-breakthrough-handheld-computer> [<https://perma.cc/BG59-U9J6>].

65. *Id.*

originally suspected it had made an error culling its own data.”⁶⁶ The article continued, “should other companies follow in Apple’s footsteps by making web access commonplace on their mobile handsets, [Google executive Vic] Gundotra believes the number of mobile searches could outpace fixed internet search ‘within the next several years.’”⁶⁷

Despite the iPhone’s breakthrough features, one crucial feature was notably missing from the iPhone: the Application Programming Interfaces (APIs), software tools that allowed programmers to enable the iOS to serve as a platform for software applications. As one reviewer noted at the time the iPhone was first released, “the only add-on software Apple is allowing will be Web-based programs that must be accessed through the on-board Web browser.”⁶⁸ Apple “says these can be made to look just like built-in programs, but the few we tried weren’t impressive.”⁶⁹

Apple’s initial reluctance to turn iOS into an application platform was not surprising, given its existing line of higher-end (and more profitable) Mac devices. Apple’s business strategy presumably was to expand into a new line of business without cannibalizing its existing one. However, Apple soon had little choice but to release APIs for iOS, after Google and other Android supporters announced that they would be releasing an open API standard for mobile devices based on Android.⁷⁰ In response, Apple announced that it, too, would release a “Software Development Kit” for application program developers that included APIs for the support of iOS software applications, including the iPhone and the iPod.⁷¹

With the release of APIs for iOS, Android, and Microsoft’s smartphone operating system, Windows CE, these mobile operating systems became applications (or “apps”) platforms. In theory, just as the browser might have evolved into a rival application platform, so too these mobile operating

66. Slash Lane, *Google iPhone Usage Shocks Search Giant*, APPLE INSIDER (Feb. 14, 2008, 12:00 PM), https://appleinsider.com/articles/08/02/14/google_iphone_usage_shocks_search_giant [<https://perma.cc/YP8C-NNRK>].

67. *Id.*

68. ALL THINGS DIGITAL, *supra* note 64.

69. *Id.*

70. *Industry Leaders Announce Open Platform for Mobile Devices*, OPEN HANDSET ALL. (Nov. 5, 2007), www.openhandsetalliance.com/press_110507.html [<https://perma.cc/VHD4-WUW3>]. The first commercial Android device was released by HTC on October 22, 2008; the first beta of the Android software development kit (“SDK”), itself the product of years of development, was released almost a year earlier, in November 2007.

71. Press Release, Apple, *Apple Announces iPhone 2.0 Software Beta* (Mar. 6, 2008), <http://www.apple.com/pr/library/2008/03/06Apple-Announces-iPhone-2-0-Software-Beta.html> [<https://perma.cc/TS9M-632J>].

systems could evolve into platforms that could support robust desktop applications that could threaten Microsoft's applications barrier to entry.

At first, the significant hardware limitations of these devices made this potential platform threat highly theoretical. In 2010, however, with the release of the iPad and the first Android tablets, iOS and Android—followed closely by Windows CE—smartphones were able to support applications and functionality that could serve as partial substitutes for a much broader array of tasks historically performed only on PCs.⁷² Although still more suited for consumption rather than content creation, and hence not direct substitutes for core desktop tasks (such as the creation and manipulation of spreadsheets or lengthy written documents), tablet sales initially skyrocketed and PC sales declined.⁷³ These tablet devices made up in portability and ease of use for other functions that previously had only been possible on desktops or laptops, but that did not require the full functionality of these devices to perform.

Both Apple and Microsoft reacted to the emerging threat posed by Android. While Google was and is a threat, Apple has generally acted on the belief that it could defend itself against IP suits by others and has chosen not to give up the substantial royalties that it can and does earn from its own licensing arrangements. The one exception was the sale of some Apple patents in 2011 to Digtude Innovations. Digtude then sued Nokia, RIM, Motorola, HTC, LG, Samsung, Sony, and Amazon for patent infringement using two Apple patents.⁷⁴

Microsoft appears to have ceded the high-end niche to Apple. Because Apple, like Microsoft, had its own existing operating system for laptops and desktops, Microsoft could expect that Apple would not continue to extend iOS to compete more directly with Windows as a desktop application platform. Although the popularity of iOS devices might enable Apple to gain some increased share for its Mac devices, Apple would not want to push iOS devices

72. David Goldman, *The End of the Desktop PC (Seriously)*, CNN (July 20, 2010, 12:55 PM), http://money.cnn.com/2010/07/20/technology/desktop_PC_death/ [https://perma.cc/YT9J-JJTH].

73. Mark Rogowsky, *The Death of the PC Has Not Been Exaggerated*, FORBES (Apr. 11, 2013, 11:30 AM), <http://www.forbes.com/sites/markrogowsky/2013/04/11/the-death-of-the-pc-has-not-been-exaggerated/> [http://archive.is/2j1vI].

74. Alex Gasser, *Digtude Files New 337 Complaint Regarding Certain Portable Communication Devices*, ITC 337 L. BLOG (Dec. 8, 2011), www.itcblog.com/20111208/digtude-files-new-337-complaint-regarding-certain-portable-communication-devices/ [https://perma.cc/ZA4J-MGU6]. A search on the USPTO's website reveals that Patents 6,208,879 and 6,456,841 were assigned to Cliff Island, LLC on August 2, 2011. They were then assigned to Digtude Innovations on Nov. 22, 2011. See Jason Kincaid, *Apple Made a Deal with the Devil (No, Worse: A Patent Troll)*, TECHCRUNCH (Dec. 9, 2011), <https://techcrunch.com/2011/12/09/apple-made-a-deal-with-the-devil-no-worse-a-patent-troll/> [https://perma.cc/WW3A-B5YL].

in a direction that would risk cannibalizing Mac device sales. The logical direction for Apple to push with its iOS devices was to position them for the consumption of content, with iPads giving way to MacBook Airs for workplace applications.

From Microsoft's perspective, Apple's pioneering of the iPhone and iPad had expanded the range of device types across which they competed, without necessarily creating a direct risk to Microsoft's desktop operating system. Rather, Microsoft could aim over time to expand its share in mainstream-priced tablets and smartphones. Absent Android, in other words, Microsoft and Apple would simply continue to compete over what were now four product categories (smartphones, tablets, laptops, desktops)—the duopolistic competition which they have maintained over the more than three decades.⁷⁵

To complete the picture, Google's strategy is particularly noteworthy. Google appears to have pursued an IP counterstrategy when in 2011 it acquired Motorola Mobility, the owner of substantial number of smartphone patents and handset technologies.⁷⁶ Google eventually (in 2014) sold the Motorola handset business to Lenovo, while maintaining the majority of the patents for defensive purposes.⁷⁷ Given Google's Android open-source driven, advertising-based business strategy, it made more sense for Google to utilize its IP portfolio for defensive purposes rather than to engage in IP privateering.

The smartphone industry has been highly dynamic. It is not surprising, therefore, that Apple's strategy has shifted from the one initially perceived by Microsoft. Apple has essentially merged iOS with Mac OS so that a consumer can transition seamlessly from device to device. Moreover, Apple is building bigger phones, bigger iPads, and smaller laptops. Also, Apple is giving away its productivity suite on all devices. Consequently, Apple is now and is likely to continue to be a threat to Microsoft as well as to Google.

75. Interestingly, PC sales have stabilized and begun to grow again, and the rate of growth of tablets has begun to decline. Apple, meanwhile, has continued to innovate in ways that take iOS devices towards consumer rather than workplace uses (most recently with the development of the Apple Watch), and hence away from Microsoft's core strength. Through mid-2014, four years after the release of the iPad, Microsoft's desktop operating system market share remains at approximately 90%, with about 8.5% for Mac and 2.3% for Linux. See NETMARKETSHARE, *supra* note 28.

76. Brian Womack, *Google Agrees to Acquire Motorola Mobility for \$12.5 Billion*, BLOOMBERG BUS. (Aug. 15, 2011, 1:58 PM), www.bloomberg.com/news/articles/2011-08-15/google-agrees-to-acquisition-of-motorola-mobility-for-about-12-5-billion [<https://perma.cc/4KH5-XQBF>].

77. Matthew Panzarino, *Google Keeps 'Vast Majority' of Motorola Mobility Patents in Sale to Lenovo*, TECHCRUNCH (Jan. 29, 2014), <http://techcrunch.com/2014/01/29/google-keeps-vast-majority-of-motorola-mobility-patents-in-sale-to-lenovo/> [<https://perma.cc/F6HU-J87G>].

Nevertheless, Microsoft's focus appears to have been on the Android threat. An initial challenge for Microsoft with Android is that Google, Android's principal corporate sponsor, does not have a substantial existing share in laptops and desktops (its Chrome operating system has only a small market share).⁷⁸ Google, therefore, could have a greater incentive to push Android in a direction that would bring it into head-to-head competition with Windows laptops and desktops. Google's workplace applications have also emerged as direct competitors to Microsoft's Office suite,⁷⁹ thereby reducing further the applications barrier to entry if Google chose to expand Android towards use on laptops and desktops.

IP privateering offered a potentially powerful tool in the highly competitive battle against Android. In the section that follows, I explore the use of that tool in the smartphone industry. First, an important warning note: just as wars can and did become heated, wars can be reduced to skirmishes, be intermittent, and they can, at least in theory, be brought to a close. In 2015 and into 2016, events began to suggest that the smartphone industry had entered a closing phase. A number of prominent patent suits had been settled and all three major smartphone OS competitors had chosen not to pursue injunctions with respect to litigation involving standards-essential patents.⁸⁰ Furthermore, Microsoft entered into a partnership agreement with Red Hat, a Linux provider, to allow customers to run enterprise versions of Linux on Microsoft's cloud-based Azure operating system.⁸¹ Most recently, Microsoft withdrew its funding of FairSearch, a third-party lobbying group which had been aggressively attacking certain travel-related aspects of Google's search algorithm.⁸²

78. Alistair Barr, *Alphabet's Google to Fold Chrome Operating System into Android*, WALL ST. J. (Oct. 29, 2015, 8:28 PM), <http://www.wsj.com/articles/alphabets-google-to-fold-chrome-operating-system-into-android-1446151134> [https://perma.cc/F5UT-KQ37].

79. Tony Bradley, *Google Offers Aggressive Incentives to Win Microsoft Office Customers*, FORBES (Oct. 19, 2015, 10:14 PM), <http://www.forbes.com/sites/tonybradley/2015/10/19/google-offers-aggressive-incentives-to-win-microsoft-office-customers/> [http://archive.is/CjIgh].

80. See, e.g., *Google Agrees to Forego Seeking Injunctive Relief for SEP Infringement as Part of FTC Settlement*, ESSENTIAL PATENT BLOG (Jan. 3, 2013), <http://www.essentialpatentblog.com/2013/01/breaking-google-agrees-to-forego-seeking-injunctive-relief-for-sep-infringement-as-part-of-ftc-settlement/> [https://perma.cc/MS9K-H5XZ].

81. See Frederic Lardinois, *Microsoft Brings Red Hat Enterprise Linux to Azure*, TECHCRUNCH (Feb. 17, 2016), <http://techcrunch.com/2016/02/17/microsoft-brings-red-hat-enterprise-linux-to-azure> [https://perma.cc/GZ7J-4K4N]; see also Janakiram MSV, *A Closer Look at Microsoft and Red Hat Partnership*, FORBES (Nov. 11, 2015, 3:06 PM), <http://www.forbes.com/sites/janakirammsv/2015/11/11/a-closer-look-at-microsoft-and-red-hat-partnership> [http://archive.is/Ppk4d].

82. Mark Bergen, *Microsoft Quietly Retreats from FairSearch, Watchdog Behind Google Antitrust Case*, RECODE (Jan. 22, 2016, 10:34 AM), <http://recode.net/2016/01/22/microsoft-quietly->

It is quite possible that the recent toning down of the strategic competitive acts described in this Article may simply be a pause and the smartphone wars will once again heat up. In either case, it is likely that this marks a milestone in the move away from competition for the desktop, with Microsoft reducing its efforts to defend its desktop OS monopoly. Either way, this raises a difficult antitrust question: how should acts of privateering be evaluated, given that the practices can change rapidly in response to changes in leadership or in industry-related technology? It is worth keeping these difficult questions in mind when reviewing the extensive history of IP privateering in light of the competitive attacks made against the open-source Android OS.

In the remainder of this Section, I complete the review of IP privateering by pointing to the role of privateering in the smartphone industry. Specifically, I discuss Microsoft's effort to consummate an outright purchase of a substantial patent portfolio—an effort that the Department of Justice blocked. Second, I describe how Microsoft, in the MOSAID, Rockstar, and Nokia transactions, expanded its privateering model. Finally, I offer some comments on Microsoft's involvement in the creation and development of Intellectual Ventures.

B. EXTENSIONS OF THE *SCO* MODEL

1. *Funding Third-Party IP Transfers: MOSAID*

Throughout the 2000s, Nokia was one of the most prominent corporate sponsors of open-source software. At one time, Nokia's Symbian operating system had been the most widely distributed open-source operating system in the world,⁸³ and Nokia, like Novell, had a substantial patent portfolio that it had pledged to use to defend open-source customers against patent claims.⁸⁴

Nokia's patent portfolio was therefore an attractive potential privateering opportunity for Microsoft. In addition to agreeing to use Windows as its primary mobile operating system, Nokia's CEO confirmed that "it is the case . . . Microsoft plus Nokia has a remarkably strong IP portfolio, and we will use

retreats-from-fairsearch-watchdog-behind-google-antitrust-cases/ [https://perma.cc/P9K6-TBS3].

83. Dena Cassella, *Symbian OS Set Free, Now Open Source*, DIGITAL TRENDS (Feb. 3, 2010, 5:21 PM), <http://www.digitaltrends.com/mobile/symbian-os-set-free-now-open-source/> [https://perma.cc/8FF2-LQER].

84. In early 2010, for example, Nokia had combined with Intel to launch the MeeGo Linux-based mobile operating system, and simultaneously pledged to protect Linux adopters against patent claims such as those that Microsoft had recently leveled against HTC and other Android OEMs. Gavin Clarke, *Nokia and Intel Defensive on MeeGo Linux Patents*, REGISTER (May 4, 2010, 9:15 PM), http://www.theregister.co.uk/2010/05/04/meego_linux_mobile_android_microsoft/ [https://perma.cc/M3DA-H74R].

that appropriately with the context of our ecosystem.”⁸⁵ As one analyst summarized, in Nokia’s “new role as Microsoft vassal . . . there’s a clear likelihood that Nokia’s many patents will be turned against Android”⁸⁶

One aspect of this agreement became apparent in September 2011 when Nokia transferred patents to MOSAID (now Conversant),⁸⁷ which had just launched a lawsuit against Linux distributors such as IBM and Red Hat.⁸⁸ Nokia later acknowledged that Microsoft, not MOSAID, had paid for the transfer.⁸⁹ Nokia received only nominal consideration from MOSAID itself (less than \$20,000).⁹⁰ Instead, MOSAID committed “to monetize the Assigned Patents and to maximize the Royalty,” and Nokia and Microsoft together would receive two-thirds of the royalties that MOSAID collected from enforcing the patents.⁹¹

Other features of the MOSAID arrangement were noted by Mark Popofsky and Michael Laufert⁹²:

- MOSAID agreed to a detailed set of confidential royalty protection provisions and milestone payments calculated to maximize the revenue MOSAID obtained from enforcement of these patents;

85. Tamlin Magee, *Swingin’ Stephen Elop Confirms Nokia-MS Deal Is About Patent Protection*, TECHEYE (Feb. 14, 2011), <http://www.techeye.net/business/swingin-stephen-elop-confirms-nokia-ms-deal-is-about-patent-protection> [https://perma.cc/42J5-YVDR].

86. Glyn Moody, *Nokiasoft: Who Are the Open Source Winners and Losers?*, COMPUTERWORLD UK (Feb. 16, 2011), www.computerworlduk.com/it-business/nokiasoft-who-are-the-open-source-winners-and-losers-3569040/ [https://perma.cc/3SFU-YK4L].

87. Ben Dummett, *Nokia Sells 2,000 Patents*, WALL ST. J. (Sept. 2, 2011), <https://www.wsj.com/articles/SB10001424053111904716604576544441441198816> [https://perma.cc/5YNK-82BQ].

88. Megan Leonhardt, *Adobe, IBM, Others Sued Over Networking Patents*, LAW360 (Aug. 11, 2011, 5:51 PM), <http://www.law360.com/articles/264173/adobe-ibm-others-sued-over-networking-patents> [https://perma.cc/4NZY-6V57].

89. Subsequent to its strategic agreement with Microsoft, Nokia engaged in at least two other patent transfers to PAEs: it transferred over 450 patents to the PAE Sisvel and more than 100 patents to the PAE Vringo. Vringo used the Nokia patents to bring two suits against Android OEM ZTE. *See Sisvel Acquires over 450 Nokia Patents, Including over 350 Patents Essential to Wireless Standards*, SISVEL (Jan. 12, 2012), <http://www.sisvel.it/news-events/news/sisvel-acquires-over-450-nokia-patents-including-over-350-patents-essential-to-wireless-standards> [https://perma.cc/84QS-9J9T]; Vringo, Inc., Current Report (Form 8-K) (Aug. 10, 2012), http://sec.gov/Archives/edgar/data/1410428/000114420412045768/v321254_8k.htm [https://perma.cc/74HR-WM4A].

90. Mark S. Popofsky & Michael D. Laufert, *Patent Assertion Entities and Antitrust: Operating Company Patent Transfers*, ANTITRUST SOURCE, Apr. 2013, at 7, http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/apr13_full_source.authcheckdam.pdf [https://perma.cc/4ZBR-LZDN].

91. *Id.* at 7–8.

92. *Id.*

- If MOSAID failed to meet its royalty obligations, Microsoft and Nokia could compel MOSAID to transfer the patents to another party for only \$10,000; and
- Microsoft retained a license that prevented MOSAID from asserting certain patents against third parties implementing certain Microsoft software in their mobile devices.

The MOSAID transaction marks an important evolution in privateering strategy. Unlike the SCO transaction described previously, in *MOSAID* Microsoft paid another company (Nokia) to transfer its IP to a third party (MOSAID). Moreover, unlike *SCO*, there was no indication that Nokia independently had been intending to use its patents to target Microsoft's downstream rivals. Finally, in *MOSAID* Microsoft was actively involved in determining the conditions under which MOSAID would receive and retain the patents, including its need to actively seek royalties (or risk forfeiting the patents) and which entities it could and should pursue. In *MOSAID*, in other words, Microsoft moved from funding third party litigation, to almost sponsoring firm's "rental" of another firm's IP for use by its agent in targeting downstream rivals.

There are three important benefits to an IP privateer with respect to a *MOSAID*-type arrangement compared to an outright acquisition. First, Microsoft had cross-license agreements in place with the majority of the Android OEMs.⁹³ By funding use of the patents without acquiring them, Microsoft ensured that the Nokia patents could be used to impose additional royalties or injunctions without falling within the scope of the Microsoft license. Second, the *MOSAID* arrangement was likely less expensive than an outright purchase. Third, MOSAID could more aggressively assert its claims than could Microsoft, especially as the intended targets of MOSAID were Microsoft customers or development partners.

2. *Organizing Privateering Consortia: Rockstar*

As noted previously, the Rockstar Consortium submitted the winning bid in the Nortel bankruptcy auction. It is notable that in Rockstar, with respect to at least one of the downstream smartphone market segments potentially covered by patents in the portfolio—mobile smartphones—the Rockstar owners comprised three of the four major downstream players in the market (Microsoft, Apple, and RIM). Their joint participation in the venture raised the

93. Press Release, U.S. Dep't of Justice, Statement of the Department of Justice's Antitrust Division on Its Decision to Close Its Investigations of Google Inc.'s Acquisition of Motorola Mobility Holdings Inc. and the Acquisitions of Certain Patents by Apple Inc., Microsoft Corp. and Research in Motion Ltd. (Feb. 13, 2012), http://www.justice.gov/atr/public/press_releases/2012/280190.htm [<https://perma.cc/MNX6-S6WF>].

prospect of horizontal downstream competitors collaborating in the assertion of intellectual property through a PAE against another downstream competitor.

With Rockstar, Microsoft had an incentive to raise the costs of its downstream Linux rivals. Moreover, unlike the Novell patents, Microsoft already had a license to the Nortel patents.⁹⁴ The Rockstar transaction was, from that perspective, more problematic than the Novell acquisition. It was also more problematic in that it was not just Microsoft that competed in the downstream market in Rockstar. Apple, RIM, and Microsoft, all co-owners of Rockstar, comprised virtually the entire market apart from Android and at the time of the acquisition were also competing.⁹⁵ These rivals collectively had a greater incentive to raise Android's costs than any one of them operating alone, and their joint management and operation of Rockstar was of greater concern.

Finally, Microsoft did not have any defensive use for the acquired patents, since dating from around 2006, Microsoft and Nortel had formed a strategic alliance which included, among other things, a perpetual worldwide cross-license for all intellectual property, including patents.⁹⁶ Indeed, the agreement with Nortel covered all Microsoft products and services, even when ownership of the patents changed hands.⁹⁷

Thus, whereas Microsoft had arguably benefited from obtaining at least a license to the Novell patents (a license which the Department of Justice authorized Microsoft to retain), the value of the Rockstar patents, apart from the ability to obtain royalties, was to either raise the costs of downstream rivals or to defend against unforeseen attacks by other patent holders. It was not surprising when, on October 31, 2013, Rockstar filed patent infringement lawsuits against Android OEMs Samsung, Huawei, ZTE, LG, HTC, Pantech, and ASUSTeK, as well as against Google search.⁹⁸

94. Press Release, Microsoft Corp., Microsoft Corporation, Nortel and Microsoft Form Strategic Alliance to Accelerate Transformation of Business Communications (July 18, 2006), <https://news.microsoft.com/2006/07/18/nortel-and-microsoft-form-strategic-alliance-to-accelerate-transformation-of-business-communications/> [<https://perma.cc/QN67-9D8B>].

95. Altogether, one advisory company estimated that Apple, RIM, Microsoft, and Android accounted for 85.4% of smartphone sales in the fourth quarter of 2011. Press Release, Gartner, Inc., Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 with 47 Percent Growth (Feb. 15, 2012), <http://www.gartner.com/newsroom/id/1924314> [<https://perma.cc/N8HP-56Q4>].

96. Press Release, *supra* note 94.

97. *Id.*

98. See Joe Mullin, *Patent War Goes Nuclear: Microsoft, Apple-owned "Rockstar" Sues Google*, ARS TECHNICA (Oct. 31, 2013, 8:10 PM), <https://arstechnica.com/tech-policy/2013/10/patent-war-goes-nuclear-microsoft-apple-owned-rockstar-sues-google/> [<https://perma.cc/4X7M-EPZZ>]. Rockstar dismissed its claims against Huawei after an undisclosed agreement;

3. *Creating the Next SCO: Nokia*

A third extension of the privateering model arose in connection with Microsoft's September 2013 acquisition of Nokia's mobile devices business. Microsoft acquired Nokia's mobile device operating assets, but Nokia retained the patents related to that business.⁹⁹ By leaving the mobile IP with Nokia, Microsoft effectively put Nokia in the same position that SCO had been relative to potential downstream targets.

In addition to converting Nokia into a PAE with respect to its mobile business, Microsoft structured a substantial part of its payment to Nokia as a "license," just as Microsoft had with SCO. Thus, Microsoft and Nokia attributed 1.65 billion euros of the purchase price to Microsoft's license to Nokia's patents¹⁰⁰—an amount that was more than three times the amount paid by Apple in 2011 for its license to Nokia's portfolio,¹⁰¹ and which greatly exceeded Nokia's reported licensing revenues over the previous several years combined.

A common feature of all of the privateering arrangements described thus far has been the separation of the IP to be asserted from the operational assets associated with it—either, as in the case of SCO and Nortel, because the operational businesses are being wound down; or, as in the case of Novell and Nokia, the asset sale is deliberately structured to separate the operational and IP assets. In Nokia, Microsoft funded the transaction without acquiring an ownership interest. Moreover, unlike both MOSAID and Rockstar, in which Microsoft maintained an oversight role, Microsoft does not appear to have attempted to maintain oversight over how Nokia would license or enforce its IP, beyond whatever terms were included in the parties' agreement and licensing arrangement.

it settled with Samsung and Google on February 2, 2015. See Aaron Vehling, *Rockets Settles with Samsung Over Search-Engine Patent*, LAW360 (Feb. 2, 2015, 2:04 PM), <https://www.law360.com/articles/617243/rockstar-settles-with-samsung-over-search-engine-patent> [<https://perma.cc/Z4AD-YHLQ>].

99. Levine, *supra* note 44.

100. *Id.*

101. Larry Dignan, *Nokia Likely Netted \$600 Million Plus in Apple Patent Settlement*, ZDNET (June 14, 2011, 8:06 PM), <http://www.zdnet.com/article/nokia-likely-netted-600-million-plus-in-apple-patent-settlement/> [<https://perma.cc/SWH2-MTSE>] (noting that although the exact payment was not disclosed to the public, a widely reported research note by Deutsche Bank analyst Kai Korschelt estimated that Nokia was likely to receive around \$608 million—at that time, a little more than 420 million euros—for the deal).

C. PRIVATEERING THROUGH INTERMEDIARIES: A ROLE FOR IV?

While Intellectual Ventures had the potential to serve as an intermediary in its privateering efforts against Android (and Apple), what is less clear is the extent to which it actually has done so. What is publicly known is that IV began to demand and obtain licensing fees from Android OEMs, including Samsung¹⁰² (the largest Android OEM) and HTC¹⁰³ in 2010 (followed by LG in 2011¹⁰⁴), around the same time that Microsoft began its own high-publicity licensing campaign against Android OEMs.¹⁰⁵

In 2011, a year after Microsoft funded the transfer of patents to MOSAID, IV brought suit against Motorola, an Android OEM (one of the first lawsuits filed by IV in its own name).¹⁰⁶ Of the six patents asserted by IV against Motorola, one notably was asserted against Apple and Microsoft before the suit was dropped and the patent purchased by a possible IV shell company.

In 2013, while its first suit against Motorola was still pending, IV brought another suit against Motorola in a different district, this time asserting seven patents.¹⁰⁷ Two of these patents were originally owned by Nokia, which transferred them in 2011 (after Nokia and Microsoft entered into their strategic partnership arrangement) to Spyder Navigations, reputedly an IV entity.¹⁰⁸

IV's pioneering role as a "patent aggregator" helped create the demand for a steady supply of patents, on one side, and PAEs to monetize them, on the other. Moreover, as the entity buying up patents from many operating

102. Ewing & Feldman, *supra* note 55, at 13, 18.

103. Press Release, Intellectual Ventures, HTC and Intellectual Ventures Announce Licensing Agreement and Strategic Alliance (Nov. 23, 2010), <http://www.intellectualventures.com/news/press-releases/htc-and-intellectual-ventures-announce-licensing-agreement-and-strategic-al/> [<https://perma.cc/333J-DA75>].

104. Nancy Gohring, *LG Signs Patent Licensing Deal with Intellectual Ventures*, COMPUTERWORLD UK (Nov. 9, 2011) <https://www.computerworlduk.com/it-vendors/lg-signs-patent-licensing-deal-with-intellectual-ventures-3317137/> [<https://perma.cc/PZR7-ZUR2>].

105. Florian Mueller, *Microsoft Announces Its 21st Android Patent Licensee, 26th known Android Patent Deal in Total*, FOSS PATENTS (Feb. 14, 2014), <http://www.fosspatents.com/2014/02/microsoft-announces-its-21st-android.html> [<https://perma.cc/DV9S-8SVR>].

106. *Intellectual Ventures I, LLC v. Motorola Mobility LLC*, 81 F. Supp. 3d 356 (D. Del. 2015).

107. *Intellectual Ventures Sues Motorola Mobility Over Patents Relating to WiFi, Cellular Standards (and Others)*, ESSENTIAL PAT. BLOG (June 19, 2013), <http://www.essentialpatentblog.com/2013/06/intellectual-ventures-sues-motorola-mobility/> [<https://perma.cc/2K9C-CK5L>].

108. Patents 6,170,073 and 7,564,784 were previously owned by Nokia. See Mike Masnick, *Intellectual Ventures Sues Google/Motorola Mobility Yet Again, Using Highly Questionable Nokia Patents*, TECHDIRT (June 20, 2013, 3:32 PM), <https://www.techdirt.com/articles/20130619/15575723536/intellectual-ventures-sues-googlemotorola-mobility-yet-again-using-highly-questionable-nokia-patents.shtml> [<https://perma.cc/T3EX-AXGV>].

companies and universities,¹⁰⁹ and packaging them for distribution to many PAEs,¹¹⁰ IV could have acted as a stand-in for Microsoft where the patents presented the opportunity for use in downstream privateering. It appears, however, that IV has not done so.

To sum up, privateering activity can raise competition questions. Indeed, it seems reasonable for Federal Trade Commission or Department of Justice reviews of acquisitions involving PAEs with substantial IP under Section 7 of the Clayton Act to include a detailed analysis of the potential implications of privateering behavior. The appropriate economic analysis of these privateering arrangements will be discussed in the sections that follow.

V. PRIVATEERING CAN RAISE RIVALS' COSTS

Although Microsoft was a pioneer in privateering, its efforts are no longer unique. In recent years, a variety of companies (the “sponsors”) have encouraged third parties to pursue intellectual property claims for the purpose of raising rivals’ costs and injuring downstream competition.¹¹¹ This IP privateering strategy has typically been accomplished by transferring patent rights to PAEs with an agreement to share royalties and other benefits flowing from patent assertion rights.¹¹²

PAEs are specialists that are often able to take advantage of their scale and experience to cut costs and to add extra value to the intellectual property that they own or control.¹¹³ Nevertheless, the rent-seeking activities that flow from the unique position of PAEs raise significant antitrust issues, the foremost of which flows from the PAEs’ ability to raise rivals’ costs. The law and economics literature make it clear that a raising rivals’ costs strategy can be an

109. Ewing & Feldman, *supra* note 55, at 7.

110. *See id.* at 7–8.

111. This will typically be accomplished when sponsors buy a financial interest in the privateering company.

112. For example, Microsoft’s agreement with MOSAID and its ownership stake in Rockstar provide it with compensation from these PAEs’ enforcement activities. *See also* Ewing & Feldman, *supra* note 55, at 13 (detailing IV’s early privateering strategy that follows the one outlined above).

113. *See* Daryl Lim, *Standard Essential Patents, Trolls and the Smartphone Wars: Triangulating the End Game*, 119 PENN. ST. L. REV. 1, 18 (2014) (noting that some PAEs connect innovators and implementing licenses, lowering transactions costs); *see also* Erica S. Mintzer & Suzanne Munck, *The Joint U.S. Department of Justice and Federal Trade Commission Workshop on Patent Assertion Entity Activities—“Follow the Money”*, 79 ANTITRUST L.J. 423, 426–427 (2014) (explaining that PAEs make settlement economical and have removed obstacles to bringing infringement suits); Joshua D. Wright & Douglas H. Ginsburg, *Patent Assertion Entities and Antitrust: A Competition Cure for a Litigation Disease?*, 79 ANTITRUST L.J. 501, 516 (2014) (characterizing the role of PAEs as redistributing economic rents along the production chain).

effective means to foreclose one or more competitors.¹¹⁴ Thus, a competitor might use such a strategy to deprive competitors of access to certain inputs or distribution channels.¹¹⁵ This could be accomplished by restricting access to valuable intellectual property or alternatively, by threatening to litigate against alleged patent infringement.¹¹⁶ A rule of reason approach is typically used to evaluate the costs and the benefits of such strategies; however, a number of commentators point to the difficulty of finding a workable balancing test.¹¹⁷

There are several notable differences between the classic analysis of raising rivals' costs and the analysis of privateering. First, the cost of engaging in a privateering strategy may be relatively low.¹¹⁸ Second, while the benefits from foreclosure may be substantial, they may not be readily apparent given the opaque nature of many privateering activities and the long-term effects of privateering.¹¹⁹ Third, the potential effectiveness of privateering by PAEs flows from information and cost asymmetries that are prevalent in technology industries. The information asymmetries arise in part because the driving force behind an IP lawsuit may not be readily apparent to the target, and even when apparent, there may be little or no reputational harm to the privateer. It may take some time for the target to ascertain the driving force behind the IP lawsuit, and even more time and effort for an enforcement theory to sort this out. A lack of substantial transparency to the costs of defending against IP-

114. See, e.g., Dennis W. Carlton, *A General Analysis of Exclusionary Conduct and Refusal to Deal—Why Aspen and Kodak Are Misguided*, 68 ANTITRUST L.J. 659, 683 (2001) (spelling out conditions under which a strategy focused on raising rivals' costs can be used to profitably extend a firm's market power in one market into a related market).

115. See, e.g., Herbert Hovenkamp, *Exclusion and the Sherman Act*, 72 U. CHI. L. REV. 147, 153–54, 160 (2005) (describing exclusionary conduct to be conduct that excludes an equally efficient rival).

116. For an example of the former, see the FTC's decision, describing a consent decree, in *In re Nielsen Holdings*. Decision and Order, *In re Nielsen Holdings N.V. & Arbitron Inc.*, FTC File No. 131-0058, Docket No. C-4439 (Feb. 28, 2014). For an example of the latter, see generally Daniel L. Rubinfeld & Robert Maness, *The Strategic Use of Patents: Implications for Antitrust*, in ANTITRUST, PATENTS AND COPYRIGHT: EU AND US PERSPECTIVES 85 (François Lévêque & Howard Shelanski eds., 2005).

117. See, e.g., Alan J. Meese, *Exclusive Dealing, the Theory of the Firm, and Raising Rivals' Costs: Toward a New Synthesis*, 50 ANTITRUST BULL. 371, 420 (2005) (explaining that a balancing analysis is outmoded and seriously flawed).

118. See Ewing, *supra* note 11, at 6. (“Outsourcing patent litigation, one branch of privateering, allows companies to shape their competitive environments and in some instances monetize their IP rights at extremely low cost.”). *But see* Matthew Sipe, *Patent Privateers and Antitrust Fears*, 22 MICH. TELECOMM. & TECH. L. REV. 191, 221 (2016) (pointing out that privateers take on substantial risk and face potential sanctions for frivolous litigation).

119. *Id.* at 203.

driven attacks is likely to deter innovative activity.¹²⁰ It also takes time and effort to sort through the potential implications of privateering-driven strategies. These costs are not only especially high when the privateering activity is secret, but they are also substantial when privateering activity are not transparent. The cost asymmetries arise to the extent that the privateer is able to expend relatively little in the way of resources while imposing substantial litigation-related costs on its competitors.¹²¹ The costs may be imposed by the threat of an injunction, by the threat of a substantial damage award, and/or by the cost of switching technologies so as to avoid patent liability in the first place.¹²²

A. PATENT HOLD UPS

Activities by PAEs are likely to involve more than rent seeking. The threat that a PAE may be successful in obtaining an injunction can force the target company to pay a relatively high royalty that would not be obtained in a hypothetical negotiation among two companies with relatively similar bargaining strengths.¹²³ As Lemley and Shapiro show, the threat of patent holdup—through the imposition of an injunction—has the potential to not only generate excessive royalties, but also to impede innovation.¹²⁴

120. See Michelle D. Miller & Janusz A. Ordover, *Intellectual Ventures v. Capital One: Can Antitrust Law and Economics Get Us Past the Trolls?*, CPI ANTITRUST CHRON., Jan. 2015, at 3, <https://www.competitionpolicyinternational.com/assets/Uploads/MillerJanuszJAN-152.pdf> [<https://perma.cc/W239-GJEL>] (“PAE[s] can diminish incentives to design-around individual technologies within [a] portfolio, thereby reducing the viability of competing technologies . . .”).

121. PAEs are in the business of monetizing IPR through litigation, and they often file several identical infringement lawsuits against different companies at the same time, which reduces their overall costs relative to the total costs of the defendants involved. Fabio Marino & Teri Nguyen, *Are Patent Trolls Now Zeroed in on Start-Ups?*, FORBES (Jan. 17, 2013, 6:24 PM), <http://www.forbes.com/sites/ciocentral/2013/01/17/are-patent-trolls-now-zeroed-in-on-start-ups/> [<http://archive.is/aPUpQ>]. For example, Rockstar filed seven identical complaints against seven different Android OEMs in the same court on the same day, which enabled them to essentially litigate a single case, while each of the defendants incur separate costs to defend the lawsuits. See Florian Mueller, *Failed \$4.4 Billion Bid for Nortel Patents Comes Back to Haunt Google and Friends on Halloween*, FOSS PATENTS (Nov. 1, 2013), www.fosspatents.com/2013/11/failed-44-billion-bid-for-nortel.html [<https://perma.cc/MV8S-2KVU>].

122. For an illustration of such an IP-driven strategy, see Rubinfeld & Maness, *supra* note 116, at 92–98, explaining how a demand for a package license for personal watercraft patents can be used to raise rivals’ costs.

123. Mark A. Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 TEX. L. REV. 1991, 1999–2009 (2007) (using an economic model to show that the threat of injunction provides the patent holder with significant leverage to bargain for more than a reasonable royalty).

124. *Id.* at 2010, 2012 (explaining that patent holdup can discourage innovation).

To illustrate, in late 2011, IV filed the first in a series of patent infringement lawsuits against Motorola Mobility relating to its use of the Android operating system.¹²⁵ Several years later, Rockstar filed a series of patent infringement lawsuits against seven different Android OEMs and requested injunctive relief in each of the lawsuits.¹²⁶ At least one of the Android OEMs (Huawei) has entered into a settlement with Rockstar, choosing to pay Rockstar an undisclosed sum for a license to its patents rather than incur the costs associated with a protracted litigation.¹²⁷

B. ROYALTY STACKING

The potential economic harms flowing from PAE activities increase when royalty stacking becomes an issue, as in the case of mobile telephony. With royalty stacking, the target faces the prospect of paying royalties on multiple claims, with any profit from selling the product being obtained only after paying all of the relevant royalties and covering other production and distribution costs. At a minimum, royalty stacking is likely to lead to increased product prices as some or all of the costs are passed on to customers.¹²⁸ With a vast number of patents at issue in a product such as a mobile phone, it is quite possible that royalty stacking will lead to more than a 100 percent increase in the downstream price of the product.¹²⁹

The higher product prices are likely to be economically inefficient for two distinct reasons. First, if the product contains multiple inputs and the input owners separately price their inputs, as is the case with smart mobile devices, there will be a “Cournot complements” problem.¹³⁰ The problem arises when

125. *Intellectual Ventures I, LLC v. Motorola Mobility LLC*, 81 F. Supp. 3d 356 (D. Del. 2015).

126. Mullin, *supra* note 98.

127. Florian Mueller, *Huawei Settles with Rockstar Consortium, Will Pay for Android's Infringement of Ex-Nortel Patents*, FOSS PATENTS (Jan. 23, 2014), <http://www.fosspatents.com/2014/01/huawei-settles-with-rockstar-consortium.html> [<https://perma.cc/LA3Z-2ZE8>].

128. See Lemley & Shapiro, *supra* note 123, at 2013 (“[H]igher running royalties will raise the downstream firm’s marginal cost, which will raise its price and thus reduce its level of output.”).

129. See Ewing & Feldman, *supra* note 55, at 12 (asserting it is theoretically possible that patent holders could extract 100% of revenue from licensee); see also Ann Armstrong, Joseph J. Mueller & Timothy D. Syrett, *The Smartphone Royalty Stack: Surveying Royalty Demands for the Components Within Modern Smartphones 2* (May 29, 2014) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2443848 [<https://perma.cc/B6CA-QXYA>] (estimating that current royalty stacking could account for over a quarter of a phone’s price).

130. The Cournot complements problem is well known in industrial organization. For a derivation, see Carl Shapiro, *Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard Setting*, in 1 INNOVATION POLICY AND THE ECONOMY 119, 119–23 (Adam B. Jaffe et al. eds., 2001).

individual input owners do not account for the negative externality that they impose on other suppliers because the input owners' higher price tends to reduce the output of the final product. When this effect is aggregated over all inputs, the result is an inefficiently low output.¹³¹ The Cournot complements problem is particularly acute when there is a royalty stacking problem.¹³²

Second, if the patents that must be licensed to make the product are individually owned, there will likely be a "double marginalization" problem, whereby each of the royalties paid on individual patents are marked up. The result is that the final price of the product will reflect multiple markups rather than the single markup that would be imposed if all patents were owned by a single entity.¹³³ This double markup would be avoided if the two firms merged to become a single vertically-integrated company.¹³⁴ By increasing any double marginalization problem, disaggregation can increase benefits of pursuing an IP privateering strategy.

While disaggregation makes sense as a business strategy for pure PAEs, the benefits of disaggregation increase further where a downstream firm is able to use the patents to privateer against a rival. According to Lemley and Melamed:

The highest bidders for at least portions of a dispersed portfolio, and therefore the likely buyers, might be practicing entities that want to use the patents to raise the costs of their rivals and are willing to pay more for the patents for their strategic value than other potential buyers that are interested solely in generating royalties. . . . Disaggregation can therefore both exacerbate the double marginalization problem and facilitate the use of patents for anticompetitive strategic purposes.¹³⁵

In Microsoft's case, the company has either distributed patents to or funded several different PAEs in its effort to target Android. These PAEs then separately seek to extract royalties from the Android OEMs. Moreover, any royalties paid by the Android OEMs to these PAEs are likely additional to the royalties Microsoft itself has already extracted from them under its Android licensing program. According to one analyst, Microsoft extracts between five

131. Lemley & Shapiro, *supra* note 123, at 2013–16 (explaining that stacking combines inefficiencies from the double marginalization problem and the Cournot-complements effect).

132. *Id.*

133. *See, e.g.,* DENNIS W. CARLTON & JEFFREY M. PERLOFF, MODERN INDUSTRIAL ORGANIZATION 415 (4th ed. 2004) (explaining how double marginalization is likely to lead to higher downstream product prices).

134. *See* Andy C. M. Chen & Keith N. Hylton, *Procompetitive Theories of Vertical Control*, 50 HASTINGS L.J. 573, 595–99 (1999) (analyzing the "successive monopoly problem").

135. Lemley & Melamed, *supra* note 52, at 2160.

and fifteen dollars from OEMs per Android device, covering seventy percent of all Android devices sold.¹³⁶

Higher prices are not the only indicator of economic inefficiency. Inefficiency also arises when an asymmetrically situated target makes strategic choices that it would not otherwise make if the threat of holdup was not credible. This inefficiency is likely exaggerated with royalty stacking when courts evaluating individual patent suits on one or more components of a product do not adequately account for the external effects of the related lawsuits on other components of the same product.¹³⁷ The inefficiency is also likely to be exacerbated to the extent that royalties are imposed on the value of the product as a whole rather than the value of the individual components.¹³⁸ Here, infringement lawsuits targeting Android OEMs necessarily seek to extract royalties based on the total value of an OEM's product (e.g., smart mobile device) because the cost of the targeted component (i.e., Android) is zero.

C. PAES AS PRIVATEERS

Privateering exacerbates the harms that are created by PAEs by transforming the PAEs into agents of third parties. Third parties, in turn, benefit when the PAEs target downstream competitors, often in a secretive

136. See Liam Tung, *Microsoft Is Making \$2bn a Year on Android Licensing – Five Times More than Windows Phone*, ZDNET (Nov. 7, 2013, 12:36 PM), <http://www.zdnet.com/article/microsoft-is-making-2bn-a-year-on-android-licensing-five-times-more-than-windows-phone/> [<http://archive.is/JwIP8>] (noting that in 2013, these Android payments totaled approximately two billion dollars).

137. Note that there is a tension between the views of the Federal Circuit and the views expressed here, which come from a competition perspective. The Federal Circuit has suggested that the effects just described are “not inappropriate” since they are the product of the monopoly right of the patent owner to exclude. See *MercExchange, LLC v. eBay, Inc.*, 401 F.3d 1323, 1339 (Fed. Cir. 2005), *vacated and remanded sub nom.* *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388 (2006).

138. To illustrate, Qualcomm charges royalties as a percentage of the price of a handset even though the vast majority of its patents read on the chipset component, and chipsets are sold separately in the marketplace. Qualcomm Inc., Annual Report (Form 10-K), at 6 (Nov. 6, 2013). Qualcomm's royalty arrangements have led both the U.S. FTC and the Korean FTC to sue Qualcomm in 2017. The FTC suit was filed in the District Court for the Northern District of California, San Jose Division, on January 17, 2017. *In re Qualcomm Antitrust Litig.*, No. 17-MD-02773-LHK, 2017 WL 5235649 (N.D. Cal. Nov. 10, 2017). On December 27, 2016 the Korean FTC announced that it was fining Qualcomm approximately \$863 million for violation of the Korean competition law. Jungah Lee & Ian King, *Qualcomm Fined \$853 Million by South Korean Antitrust Agency*, BLOOMBERG (Dec. 27, 2016, 10:38 PM), <http://www.bloomberg.com/news/articles/2016-12-28/qualcomm-fined-853-million-by-south-korea-s-antitrust-agency-ix8csvth> [<https://perma.cc/7ZHF-5FNY>].

manner.¹³⁹ Of course, the principal-agent relationship between the sponsor and the PAE is not perfect, especially when the sponsor has no financial interest in the PAE. However, the technological world in which the sponsors and PAEs operate has important elements of a repeated game. Given the potential to acquire future IP from the sponsor, the PAE has a long-term interest to operate with the welfare of the sponsor in mind. Conversely, the sponsor will benefit if the PAE becomes, through learning, more and more efficient in asserting patents that will advantage the sponsor.

While the results of privateering are similar in character to the results flowing from the actions of PAEs as implementing licensees, important differences exist. First, the secrecy as to which company is driving the PAEs' actions against downstream competitors increases the likelihood that targeting a particular competitor will be successful. The benefits to the firm that is sponsoring such a PAE arise from the change in the downstream competitive environment. Second, the time and effort involved in tracking the entity behind the lawsuit will raise the costs of responding to the lawsuit, delay countermeasures, and ultimately will discourage possible settlements that will remove impediments to innovation. A route to prompt settlement should be preferred not only because it eliminates the cost of time-consuming litigation, but also because it would move closer to the traditional world in which a licensing arrangement between two willing parties is negotiated.

In essence, privateering benefits the PAEs, which collect funds through patent settlements, damage awards, and royalties. Moreover, privateering benefits the sponsor of the activity whose competitive position has been improved. As a result, the encouragement of PAEs as agents by a sponsoring principal has the potential to be a highly effectively means of exclusion.¹⁴⁰ The cost to the company that is putting into effect such a strategy may be modest, and can be substantially less than the competitive harm that can be inflicted upon rivals. The costs imposed downstream that flow from the use of

139. When acting as agents in principal-agent relationship, PAEs are sometimes described as “hybrid PAEs.” To our knowledge, the term was coined by Carl Shapiro at a joint workshop hosted by the Federal Trade Commission and the Antitrust Division of the U.S. Department of Justice. See Carl Shapiro, Patent Assertion Entities: Effective Monetizers, Tax on Innovation, or *Both?*, Presentation at the U.S. Department of Justice Antitrust Division 4 (Dec. 10, 2012), <https://www.justice.gov/sites/default/files/atr/legacy/2013/07/14/290074.pdf> [<https://perma.cc/Z55Y-Q7YR>]. For a brief discussion of the competition issues, see Ewing & Feldman, *supra* note 55, at 26–28. See also Morton & Shapiro, *supra* note 29, at 489–91.

140. This possibility was recognized by Lemley and Melamed in their groundbreaking “Forest for the Trolls” article. Lemley & Melamed, *supra* note 52, at 2145. According to the authors, “[t]heir objective is to impose royalty costs on competitors that will reduce demand for the competitor’s products and thereby increase demand for their own products. . . . In effect the[y] . . . are willing, for strategic reasons, to charge supramonopoly prices . . .” *Id.*

privateering as an exclusionary device are likely to be especially high in the mobile telephony industry. Mobile devices have an array of components and features that read on a vast number of patents and which depend on multiple standard-setting organizations to achieve interoperability.¹⁴¹ The need for interoperability is likely to increase the number of complementary inputs and consequently to increase the costs flowing from the Cournot complements problem.¹⁴²

D. AN INNOVATION TAX

Privateering lawsuits brought by PAEs will in some cases represent a battle over economic rents between two symmetrically-situated entities. Even in this case, however, these lawsuits can generate substantial economic inefficiencies. Not only is the proliferation of lawsuits socially costly, but the suits act as a tax on innovation, and any reduction in innovation will reduce social welfare.¹⁴³ Indeed, the potential dynamic cost of lost economic growth has the potential to greatly exceed any static costs of litigation.¹⁴⁴

To understand the implications of this “innovation tax,” it is useful to view patent infringement suits that are directed against the Android operating system as imposing a cost on competitors that is more or less independent of the value of the handset that incorporates the OS. In essence, privateering-driven patent infringement suits impose a specific tax on competitors’ products. A portion of the cost of the tax will be borne by the competitors and a portion will be passed on to downstream customers.¹⁴⁵ Moreover, competitors bear the greatest burden when demand is relatively elastic. As a result, it is the OEMs that offer products at the low end of the handset spectrum that will bear the greatest burden. (Customers at the low end are the most price sensitive and have the most elastic demand for handsets.) In the smart mobile devices market, OEMs that manufacture devices at the low end of the handset spectrum are predominantly producers of Android devices.

141. See Lim, *supra* note 113, at 20 (2014); Mark A. Lemley, *Ten Things To Do About Patent Holdup of Standards (and One Not To)*, 48 B.C. L. REV. 149, 150 (2007).

142. For a detailed discussion of these implications in a world of “thick” patents, see Robert G. Harris, *Patent Assertion Entities & Privateers: Economic Harms to Innovation and Competition*, 59 ANTITRUST BULL. 281, 285–93 (2014).

143. See Ewing & Feldman, *Giants*, *supra* note 55, at 25.

144. See Shapiro, *supra* note 139 (pointing to the importance of innovation in driving economic growth). For evidence of harm to innovation, see Catherine Tucker, *Patent Trolls and Technology Diffusion: The Case of Medical Imaging* (Apr. 14, 2014) (unpublished manuscript), <http://ssrn.com/abstract=1976593> [<https://perma.cc/V6HY-73U9>].

145. See ROBERT S. PINDYCK & DANIEL L. RUBINFELD, *MICROECONOMICS* 355 (9th ed. 2017).

In general, the imposition of a specific tax leads to a reduction in the quantity supplied by the taxed entities and a reduction in the aggregate quantity sold in the market as a whole.¹⁴⁶ Hence, the obvious exclusionary impact of privateering practices is that it raises rivals' costs. However, there is a more significant effect—the strategy serves as a pure tax on innovation. To see why, consider the investment decision of a risk-averse venture capitalist seeking to invest in technology. The “privateering tax” reduces the return on an investment in a company that offers a competitive OS or a partial substitute to the Microsoft OS. All things equal, the lower return will encourage the venture capitalist to look elsewhere. Moreover, given that the magnitude and the targets of the tax are likely uncertain, the tax will increase risk. Moreover, this risk is effectively nondiversifiable, since the only way in which competitors can reduce or eliminate the risk is by not making the OS investment in the first place.¹⁴⁷

I agree with Scott Morton and Shapiro that privateering is likely to deter innovation and harm consumers. The biggest concerns are (1) the reduction in the downstream firm's investment in its own products due to payments to the PAE; (2) the loss of consumer benefits resulting from the reduction in the downstream firm's investments in its own products; and (3) the share of the cost the PAE imposes on the downstream firm that goes to cover legal fees and other transaction costs.

To sum up, the evaluation of competitive issues relating to innovation is inherently difficult, given that investments in research and development vary widely from company to company and from industry to industry.¹⁴⁸ While some (e.g., Schumpeter) have emphasized innovation by firms with substantial

146. *See id.*

147. For a basic introduction to risk and investment, see *id.* at 583–86. For an analysis of how one enforcement agency has accounted for innovation issues in its evaluation of merger and non-merger activity, see generally Daniel L. Rubinfeld & John Hoven, *Innovation and Antitrust Enforcement*, in DYNAMIC COMPETITION AND PUBLIC POLICY: TECHNOLOGY, INNOVATION, AND ANTITRUST ISSUES 65 (Jerry Ellig ed., 2001).

148. For a thorough discussion of these issues, see Herbert Hovenkamp, *Antitrust and Innovation: Where We Are and Where We Should Be Going*, 77 ANTITRUST L.J. 749 (2011). According to Hovenkamp, “just as innovation promises greater growth than market movements toward competition, so too can *restraints* on innovation do more harm.” *Id.* at 751.

market power,¹⁴⁹ others (e.g., Arrow) have pointed to the innovation-related benefits that flow from competition.¹⁵⁰

Regardless of one's view about the relationship between market structure and innovation, there can be no doubt that the long-term adverse effects of an innovation tax are likely to dwarf any purely short-term exclusionary effects. Assume for example, that the real (quality-adjusted) output in the mobile telephony industry is expected to grow at eight percent per year. At this rate, handset output will double in eight years. However, if the "privateering tax" adversely affects innovation so as to reduce the growth rate to seven percent, it will take over nine years for handset output to double. For this reason, a number of commentators have stressed the importance of dealing with anticompetitive restraints on innovation.¹⁵¹

VI. ANTITRUST IMPLICATIONS OF PRIVATEERING

Although Microsoft has been a systematic user, privateering is a practice that has been used by Nokia, Apple, and a number of other technology-driven companies. For example in 2013, Ericsson sold 2,185 phone-related patents and applications to Unwired Planet, Inc., a licensing company.¹⁵² About the same time, BT Group and Alcatel-Lucent transferred patent rights to several patent-licensing entities.¹⁵³

149. Thomas A. Piraino, Jr., *Identifying Monopolists' Illegal Conduct Under the Sherman Act*, 75 N.Y.U. L. REV. 809, 817 (2000) ("Schumpeter believed that the potential for superior returns gives firms an incentive to develop new products in their quest for monopoly power; furthermore, the fear of losing such power guarantees . . . innovation even after they have achieved a monopoly.").

150. Jonathan B. Baker, *Beyond Schumpeter vs. Arrow: How Antitrust Fosters Innovation*, 74 ANTITRUST L.J. 575, 578 (2007) ("[A] monopolist might innovate less than competitive firms because a monopolist has less to gain.").

151. See, e.g., Herbert Hovenkamp, *Restraints on Innovation*, 29 CARDOZO L. REV. 247, 253–54 (2007) (explaining that restraints on innovation very likely produce greater economic harm than restraints on competition).

152. Ingrid Lunden, *Unwired Planet Has Bought 2,400+ Wireless Patents from Ericsson to Beef Up Its Patent Fights Against Google, Apple and RIM*, TECHCRUNCH (Jan. 10, 2013), <http://techcrunch.com/2013/01/10/unwired-planet-has-bought-2400-wireless-patents-from-ericsson-to-beef-up-its-patent-fights-against-google-apple-and-rim/> [https://perma.cc/YY76-C8M3].

153. See Susan Decker, *Patent Privateers Sail the Legal Waters Against Apple, Google*, BLOOMBERG (Jan. 10, 2013, 9:00 PM), <http://www.bloomberg.com/news/articles/2013-01-11/patent-privateers-sail-the-legal-waters-against-apple-google> [https://perma.cc/7VYF-AAYD]; see also Joff Wild, *Alcatel Agrees Privateering Hook-Up with Vringo; Expect More Such Deals to Follow*, IAM BLOG (Dec. 2, 2013), www.iam-media.com/blog/detail.aspx?g=ada129d1-6957-46ed-8bf4-3c068cb5690d [https://perma.cc/7EYF-CZ4D].

The competitive concerns associated with privateering could become a pervasive problem in connection with the antitrust agencies' review of patent acquisitions because, as noted in Section V.B, practicing entities have a strong incentive to use privateering to raise rivals' costs, such that they may be willing to outbid other parties "that are interested solely in generating royalties."¹⁵⁴

It would therefore be a substantial policy concern if IP privateering were deemed to fall within the interstices of effective antitrust enforcement. Enforcement could come from the Sherman Act, which under Section 1 prohibits contracts and combinations in restraint of trade and under Section 2 treats as unlawful the monopolization or attempt to monopolize a relevant market.¹⁵⁵ Alternatively, it could come from Section 7 of the Clayton Act, which constrains merger, acquisitions, and joint ventures that substantially lessen combination.¹⁵⁶ There are three characteristics of IP privateering that might raise evidentiary or legal hurdles: (1) the use of IP litigation as part of the anticompetitive scheme; (2) the attribution of the PAE's conduct to the sponsor; and (3) the ability to show the requisite anticompetitive effects. In most instances, however, these characteristics do not pose insurmountable barriers to effective enforcement, for the reasons set out below.

A. NOERR-PENNINGTON CONCERNS

The *Noerr-Pennington* doctrine poses some obstacles to effective enforcement, which can be overcome by the line of argument described below. One of the steps in the implementation of any IP privateering scheme is either the initiation of IP litigation or licensing activity that takes place in the shadow of potential litigation. Under the *Noerr-Pennington* doctrine, a genuine effort to obtain governmental action, where that action would have an anticompetitive effect, is deemed to fall outside the scope of actionable conduct under the Sherman Act.¹⁵⁷ As the FTC stated in a staff report on the *Noerr-Pennington* doctrine in 2006, "although the Court has not provided a consistent source for the doctrine, it appears to be rooted in a construction of the Sherman Act to avoid conflict with the constitutional right to petition the government for

154. Lemley & Melamed, *supra* note 52, at 2160

155. See Zachary C. Flood, *Antitrust Enforcement in the Developing E-Book Market: Apple, Amazon and the Future of the Publishing Industry*, 31 BERKELEY TECH. L.J. 879, 895–96 (2016).

156. See Cassandra E. Havens, *Saving Patent Law from Competition Policy and Economic Theories: Kimble v. Marvel Entertainment*, 31 BERKELEY TECH. L.J. 371, 376 (2016).

157. FED. TRADE COMM'N, ENFORCEMENT PERSPECTIVES ON THE NOERR-PENNINGTON DOCTRINE 6 (2006), <https://www.ftc.gov/sites/default/files/documents/reports/ftc-staff-report-concerning-enforcement-perspectives-noerr-pennington-doctrine/p013518enfperspectnoerr-penningtondoctrine.pdf> [<https://perma.cc/QP95-S4W3>].

redress of grievances and the principle of effective government decision-making.”¹⁵⁸

In *California Motor Transport Co. v. Trucking Unlimited*, the Court held that access to the courts and administrative agencies is an aspect of the right to petition, and hence *Noerr*'s protection generally extends to administrative and judicial proceedings, as well as to efforts to influence legislative and executive action.¹⁵⁹ The Court also found, however, that the specific conduct of the complaint fell under the “sham” exception to *Noerr*.¹⁶⁰ In its later decision in *Professional Real Estate Investors, Inc. v. Columbia Pictures Industries, Inc.* (“*PRE*”), the Court held that, when applied to a single lawsuit, a case does not constitute a “sham” unless it satisfies a two-part test: (1) the lawsuit must be “objectively baseless” in the sense that no reasonable litigant could realistically expect success on the merits; and (2) the suit must reflect a subjective intent to use the governmental process—as opposed to the outcome of that process—as an anticompetitive weapon.¹⁶¹

IP privateering appears to meet the second part of *PRE*'s two-part test: it is designed to raise the costs of the privateering sponsor's rival, not to achieve success on the merits. The inherent ambiguity of intellectual property claims, however, could make it difficult to meet the first part of the *PRE* test. Where there has only been a single case with no transfer of IP assets or other property—as, for example, in the *SCO* case that Microsoft funded against Linux customers—the *Noerr-Pennington* doctrine could prove to be a hurdle to a Sherman Act claim.¹⁶²

Most IP privateering appears to involve both the transfer of assets and more than a single case. Consider, for example, a simple fact pattern where an IP privateering sponsor breaks up its patent portfolio into three complementary bundles and transfers two of the bundles to PAEs for the purpose of asserting them (or seeking to license them) to the sponsor's rival. As Lemley and Melamed note, “agreements to sell or disperse patents that

158. *Id.*

159. *Cal. Motor Transp. Co. v. Trucking Unlimited*, 404 U.S. 508, 510–11 (1972).

160. *Id.* at 516.

161. *Prof'l Real Estate Inv'rs, Inc. v. Columbia Pictures Indus., Inc.*, 508 U.S. 49, 60–61 (1993).

162. The same would be true of non-IP based lobbying efforts, as for example, Foundem's 2010 campaign against Google, supported by the Microsoft-backed Initiative for a Competitive Online Marketplace. See Danny Hakim, *Microsoft, Once an Antitrust Target, Is Now Google's Regulatory Scold*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/technology/microsoft-once-an-antitrust-target-is-now-googles-regulatory-scold.html [<https://perma.cc/S46R-JYZB>] (identifying Microsoft as the founder of the lobbying group, Initiative for a Competitive Online Marketplace). For a view that *Noerr-Pennington* “almost certainly immunizes privateering activity,” see Sipe, *supra* note 118, at 203.

seem likely to create or exacerbate a double marginalization problem could be challenged under both Sections 1 and 2 of the Sherman Act and Section 7 of the Clayton Act,” especially “if one or more of the entities involved is likely to have strategic incentives to impose costs on rivals.”¹⁶³ They explain:

An antitrust violation might be established . . . if the disaggregation is likely to increase costs to rivals of one or both of the parties to the transaction or their customers and thereby to injure competition in a downstream market in which the technologies claimed by the affected patents are used¹⁶⁴

In this analysis, it is the *asset transfer*, not the subsequent assertion of the patents in litigation, that is competitively problematic and could be found unlawful under Clayton Act analysis as having an effect that is likely to substantially lessen competition. As the FTC staff concluded:

Viewed in its entirety, the case law provides ample room to conclude that, outside of the political arena, a pattern of repetitive petitions filed without regard to merit and for the sole purpose of using the government process, rather than the outcome of the process, to harm directly marketplace rivals and suppress competition should be subject to antitrust liability In addition, sound policy reasons support treating repetitive use of the government process against rivals differently from single lawsuits.¹⁶⁵

Thus, antitrust law may indeed provide a remedy for the anticompetitive effects of IP privateering.

B. ATTRIBUTING ACTIONS OF PAE AGENTS TO THE PRIVATEERING SPONSOR

A second potential hurdle is an evidentiary one. It is possible that in some instances a privateering sponsor’s transfer of patents to a PAE is a sham and the privateering sponsor really directly controls the PAE. Such instances are “unlikely to be common, however, because such a sham transaction would be too likely to be detected and punished, either by the target or by antitrust law.”¹⁶⁶ Instead, the privateering sponsor is likely to exercise control by constraining the incentives of the PAE, either directly through contract or indirectly by directing the PAE’s activities towards the sponsor’s rival.¹⁶⁷ As an example of the latter, Lemley and Melamed give a hypothetical that appears to

163. Lemley & Melamed, *supra* note 52, at 2179.

164. *Id.* at 2179 n.257.

165. FED. TRADE COMM’N, *supra* note 157, at 35.

166. Lemley & Melamed, *supra* note 52, at 2160–61.

167. *See id.* at 2137–38.

have been inspired by Rockstar: “For instance, if Microsoft were to sell to a troll a smartphone patent that was already licensed to Apple and to users of the Microsoft and Blackberry operating systems, the only significant remaining target for such a patent would be phones using the competing Android operating system.”¹⁶⁸

In instances where the sponsor’s control is short of outright ownership, it raises the question of whether the PAE’s conduct fairly can be attributed to the sponsor. As a matter of principle, Ewing has argued that “in those instances where a sponsor would not have been privileged to use [its] own IPRs against the target on anticompetitive grounds, then the sponsor should not be allowed to privateer against the target using third-party IPRs either.”¹⁶⁹ In arguing for this attribution rule, Ewing notes that “IP privateering adds to the IPRs at the disposal of the sponsor, thus making the sponsor even more anticompetitive than if its own IPRs had been used.”¹⁷⁰

As noted earlier, it is much harder for the target to protect against IP privateering than against an intellectual property claim by the sponsor itself. If Microsoft had kept the Novell patents in the CPTN transaction, it would have been much easier for Android OEMs or Google to defend against Microsoft’s assertion of the patents than it was for them to defend against patents in the hands of MOSAID or Rockstar: they might have already obtained licenses to Microsoft patents or have been able to bring a counterclaim against Microsoft. As a matter of policy, therefore, IP privateering conduct should be more susceptible, not less, to challenge than would the sponsor’s outright acquisition of the intellectual property in question.

Certainly as a matter of Clayton Act enforcement, it should be possible for the agencies to adopt a rule that, when a company helps to fund the transfer of intellectual property to a third party, there will be a rebuttable presumption that it controls that third party. This would raise the cost of litigation for the asserting party and could discourage inefficient litigation. An even greater challenge than Rockstar-like transactions, however, are transfers such as the flow of patents through entities like IV, where the mechanism of control, as between Microsoft and IV, might be extremely difficult to disentangle. A privateering effort should not avoid liability simply on the basis of the difficulty of its discovery. There may be little choice but to disentangle these relationships if anticompetitive privateering is to be adequately evaluated and (when appropriate) deterred.

168. *Id.* at 2161.

169. Ewing, *supra* note 11, at 80.

170. *Id.*

C. SUBSTANTIVE ANTITRUST ISSUES

There is arguably some justification for IP privateering, based on the efficiencies created by the IP-litigation specialists. However, the potential harms are great. IP privateering might enable the privateering sponsor, by making multiple patent assertions through different entities, to claim patent damages beyond what the sponsor reasonably could expect if the patents were held and asserted by a single entity. It could also be a means by which the privateering sponsor avoids FRAND obligations; or it could enable the privateering sponsor to raise costs to the sponsor's rival or its customers.¹⁷¹

None of these purposes should be encouraged. Where there is evidence of anticompetitive effect—that is, evidence that the sponsor's purpose in engaging in this privateering is to raise its rivals' costs, and evidence that such increased costs are the likely outcome of the sponsor's conduct—such evidence should be viewed in light of the broad scope of the Clayton and Sherman Acts. For example, in 2012 Intellectual Ventures brought a lawsuit against Motorola Mobility (a Google, Inc. division), claiming that Google's Motorola smartphone software patents infringed a number of IV's patents. A successful case would have advantaged the Microsoft and Apple smartphone operating systems. That case was settled after the jury failed to reach an agreement.¹⁷²

Because patent transactions often raise the question whether the patents involved are “blocking” patents (patents that are essential to make a particular technology or device workable), it could be easy to mistake the absence of blocking patents in an IP privateering transfer for a lack of likely anticompetitive effects. While it may have foreclosure implications, IP privateering is not a classic foreclosure strategy—it is fundamentally a strategy oriented around raising rivals' costs. Indeed, as noted above, IP privateering is indifferent to the quality of the underlying patents. The goal is to make repeated claims that stack royalties and deter rivals' customers, not to block particular products from the market.

VII. CONCLUSIONS

The legal and evidentiary difficulties inherent in bringing an antitrust action against PAEs and their sponsors should not rule out enforcement, especially

171. See, e.g., Michael Mattioli, *Patent Pool Outsiders*, 33 BERKELEY TECH. L.J. (forthcoming 2018) (describing how Lucent assigned its patents to a trust in order to avoid FRAND obligations arising from its joinder of the MPEG-2 patent pool).

172. Dan Levine, *Google, Intellectual Ventures Case Over Patents Ends in U.S. Mistrial*, REUTERS (Feb. 5, 2014, 4:30 PM), <http://www.reuters.com/article/us-google-iv-mistrial/google-intellectual-ventures-case-over-patents-ends-in-u-s-mistrial-idUSBREA1500Y20140206> [<https://perma.cc/N7ZZ-VYZG>].

when seen in the context of acquisitions falling within the purview of Clayton Section 7. Companies can use IP privateering to foreclose rivals and raise their costs precisely because of the difficulties in detection and prosecution, and antitrust agencies should especially take into account the prospect of such conduct.

While this Article has emphasized antitrust concerns, it is worth asking whether there are remedies within the IP space that might reduce the incentives to engage in inefficient privateering activity. Solely for purposes of discussion, I suggest two avenues for further inquiry. First, part of the problem flowing from privateering arises because many privateering arrangements are opaque. A requirement that new assignees be made public when certain IP is transferred could prove beneficial. To avoid excessive and unnecessary costs, such a requirement would need to be limited either (1) to particular industries, such as telecommunications or pharmaceuticals; or (2) to IP whose value is believed to exceed an appropriate threshold.¹⁷³

Second, when IP transfers are partial, it is relatively difficult to sort out the interests of the parties and to foresee the economic implications of any privateering activity that might ensue. A requirement that partial assignments of IP be made available to the competition agencies under conditions similar to the antitrust enforcement agencies requirements with respect to joint ventures would be desirable.¹⁷⁴ The Patent Trial and Appeal Board (“PTAB”) seems to be taking a similar requirement seriously by declining to institute petitions where the “real parties in interest” are not properly named.¹⁷⁵ Adding clarity to the acts of privateers is likely to increase the likelihood that IP disputes will be settled.¹⁷⁶

173. See Peter S. Menell & Michael J. Meurer, *Notice Failure and Notice Externalities*, 5 J. LEGAL ANALYSIS 1, 42 (2013) (noting the requirement could be enforced by a cap on damages when there is a failure to make the arrangement public).

174. See generally FED. TRADE COMM’N & U.S. DEP’T OF JUSTICE, ANTITRUST GUIDELINES FOR COLLABORATIONS AMONG COMPETITORS 25–27 (2000), www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf [https://perma.cc/VD6J-DEAP] (referencing the filing requirement of the Horizontal Merger Guidelines, while pointing to a number of safety zones). The publication of the licensees should also be considered.

175. See Leahy-Smith America Invents Act, Pub. L. No. 112-29, § 312(a)(2), 125 Stat. 284 (2011). The availability of a PTAB review depends heavily on the willingness of district court judges to grant a stay of litigation pending a review.

176. It is well known that disputes are more likely to be settled, other things equal, the closer the parties’ expectations about the likelihood that the plaintiff will succeed on the merits. See, e.g., Robert D. Cooter & Daniel L. Rubinfeld, *Economic Analysis of Legal Disputes and Their Resolution*, 27 J. ECON. LITERATURE 1067, 1076 (1989).

AT THE PRIVACY VANGUARD: CALIFORNIA'S ELECTRONIC COMMUNICATIONS PRIVACY ACT (CALECPA)

Susan Freiwald[†]

ABSTRACT

This Article engages with and contributes to the academic literature on electronic communications privacy by providing the first detailed assessment of California's groundbreaking legislation. It provides judges and practicing attorneys with practical information on how to interpret and apply CalECPA. In addition, because it analyzes the statute's innovations and the questions it leaves unanswered, those considering whether to replicate CalECPA's provisions in Congress, as well as statehouses across the country, will find it valuable.

DOI: <https://doi.org/10.15779/Z388G8FH73>

© 2018 Susan Freiwald.

[†] Professor, USF School of Law. I owe thanks to Mario Iskander, Everett Monroe, Arlette Noujaim, and Chi Vu for their excellent research assistance and Chris Conley, Nicole Ozer, Lee Tien, and attendees of the Privacy Law Scholars' conference in June of 2016 for their exceptionally helpful editing suggestions and discussions about CalECPA. I served as an issue expert for CalECPA's authors, State Senators Mark Leno and Joel Anderson, and as a member of the bill's policy and language teams. In that capacity, I helped answer questions about the bill's language, testified at legislative committee hearings about its legal impact, and coordinated dozens of academic colleagues to send a scholarly support letter to California Governor Jerry Brown.

TABLE OF CONTENTS

I.	INTRODUCTION	133
II.	WHAT IS CALECPA AND HOW DID IT GET PASSED?	134
	A. CALIFORNIA LAW.....	136
	B. FEDERAL LAW.....	139
	C. CALECPA'S PASSAGE.....	143
III.	CALECPA'S PROVISIONS	147
	A. WHO AND WHAT DATA IS PROTECTED?.....	147
	1. <i>Who Is Protected?</i>	147
	2. <i>What Is Protected?</i>	148
	3. <i>What Is Not Protected?</i>	149
	B. WHO MUST COMPLY?.....	150
	C. HOW TO COMPLY?.....	151
	1. <i>Warrant-Regulated Methods</i>	151
	2. <i>Warrant Requirements</i>	153
	3. <i>Exclusions from the Warrant Requirement</i>	155
	4. <i>Voluntary Disclosures and Consent</i>	157
	5. <i>Emergency Provisions</i>	159
	6. <i>Notice Requirements</i>	159
	D. SANCTIONS AND REMEDIES.....	161
IV.	WHAT SETS CALECPA APART FROM FEDERAL LAW	162
	A. CALECPA VERSUS FEDERAL WIRETAP AND PEN REGISTER LAW.....	163
	1. <i>Wiretap Law Differences</i>	163
	2. <i>Pen Register Law Differences</i>	163
	B. CALECPA COMPARED TO THE STORED COMMUNICATIONS ACT (SCA).....	164
	1. <i>Who Is Protected?</i>	164
	2. <i>What Is Protected and How to Comply</i>	164
	3. <i>Notice</i>	168
	4. <i>Sanctions and Remedies</i>	169
V.	CONSIDERATIONS GOING FORWARD—FOR CALECPA AND SIMILAR LAWS	170
	A. OPEN ISSUES.....	170
	B. IMPACT ON BROADER LEGAL QUESTIONS.....	174
VI.	CONCLUSION	175

I. INTRODUCTION

In a significant and somewhat surprising development, the law governing access to electronic communications by law enforcement in California became much more protective of communications privacy a few years ago in 2016. The California Electronic Communications Privacy Act (CalECPA)¹—the most privacy-protective legislation of its kind in the nation²—came into effect on January 1, 2016.³ In many ways, CalECPA simplified electronic surveillance law in California by making it more uniform, but those lawyers, judges, and companies affected by it would benefit from clarification of its potentially confusing provisions.⁴ Moreover, it makes sense to review what makes CalECPA a worthy model, as some states have patterned reform bills on CalECPA,⁵ and other states and even Congress may want to do the same.⁶ This Article explains CalECPA’s intricate provisions, including how it significantly improves on federal law. It heralds the new law’s statutory innovations and

1. California Electronic Communications Privacy Act, CAL. PENAL CODE § 1546 (West 2017).

2. Kim Zetter, *California Now Has the Nation’s Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), <https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/> [<http://perma.cc/DL9B-GTXH>].

3. Governor Brown signed the bill, S.B. 178, into law on October 8, 2015. *In a Landmark Victory for Digital Privacy, Gov. Brown Signs California Electronic Communications Privacy Act into Law*, ACLU OF N. CAL. (Oct. 8, 2015), www.aclunc.org/news/landmark-victory-digital-privacy-gov-brown-signs-california-electronic-communications-privacy [<http://perma.cc/YN5W-KS6X>].

4. Just after CalECPA’s passage, lawyers offered companies help in understanding the new law’s requirements. *See, e.g.*, Abby Liebeskind, *8 Things to Know About CalECPA*, ZWILLGEN BLOG (Dec. 4, 2015), <http://blog.zwillgen.com/2015/12/04/8-things-to-know-about-calecpa/> [<https://perma.cc/M79Z-4WXT>]. Law enforcement agencies described the new law as needing clarification. *See, e.g.*, Mark Hutchins, *Electronic Communications Searches: The New California Law*, POINT VIEW, Winter 2016, at 2, http://le.alcoda.org/publications/point_of_view/files/POV_Winter_2016.pdf [<http://perma.cc/U398-JU4H>] (referring to “uncertainties and dubious provisions” in CalECPA).

5. *See, e.g.*, Assemb. B. No. 1895, 2017–2018 Gen. Assemb., 1st Reg. Sess. (N.Y. 2017) (basing the provisions of the “New York Electronic Communications Privacy Act” on CalECPA); S.B. 61, 1st Reg. Sess. (N.M. 2017) (basing provisions of the “Electronic Communications Privacy Act” on CalECPA).

6. *See, e.g.*, Chris Conley, *California Leads on Electronic Privacy: Other States Must Follow*, ACLU: SPEAK FREELY (Oct. 13, 2015, 5:15 PM), <https://www.aclu.org/blog/speak-freely/california-leads-electronic-privacy-other-states-must-follow> [<http://perma.cc/WG65-KQMQ>]; G.S. Hans, *California ECPA Coalition Looks to Modernize Email Privacy*, CTR. FOR DEMOCRACY & TECH. BLOG (Feb. 9, 2015), <https://cdt.org/blog/california-ecpa-coalition-looks-to-modernize-email-privacy/> [<http://perma.cc/P6QQ-ZR3C>] (“As the most populous state and a key influencer on privacy issues, California addressing this pressing issue with strong language will help advance federal reform efforts.”).

also identifies some of the complex questions in communications privacy law that CalECPA currently leaves unresolved.

The Article is organized in six parts. Part II describes CalECPA's passage. It lays out the legal backdrop for the bill and shows how its proponents used that backdrop to argue that CalECPA was both much needed and, at the same time, not a big stretch from current law. In addition, it identifies a social context of increased concern about online privacy that likely contributed to the bill's passage.⁷ Part III carefully reviews each of CalECPA's chief provisions, describing what they do and how they interact with each other and with other parts of the California code. Part IV describes how CalECPA improves upon its namesake, the federal Electronic Communications Privacy Act (ECPA),⁸ by illustrating CalECPA's expansiveness and its additional protections. Part V identifies some of the legal issues that CalECPA leaves open, issues that other states and Congress might well consider, and it suggests several ways that CalECPA may challenge the way judges, lawmakers and scholars think about electronic communications privacy. Part VI concludes.

II. WHAT IS CALECPA AND HOW DID IT GET PASSED?

CalECPA replaced a number of California state statutes that offered complex and incomplete protections with a relatively uniform approach that requires law enforcement⁹ to obtain a warrant to access almost all electronic communication information.¹⁰ To comply with CalECPA, government entities in California must obtain a circumscribed warrant based on probable cause before they may obtain a person's electronic communication information from either her service provider or her electronic device.¹¹ As Part IV explains in more detail, CalECPA goes much further than ECPA by requiring a warrant for access to all electronic communications content, not just a subset of it, and

7. See, e.g., Eyrason Eidam, *California's New Law Affects Search Warrants for Electronic Communications, Data—But How Much?*, GOV'T TECH. (Jan. 6, 2016), <http://www.govtech.com/state/Californias-New-Law-Affects-Search-Warrants-for-Electronic-Communications-Data-But-How-Much.html> [<http://perma.cc/PGT4-7K3B>] (reporting that disclosures of National Security Agency surveillance had heightened concern about digital data collection and that CalECPA was an “impassioned issue”).

8. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

9. CalECPA applies to all government entities but will chiefly regulate law enforcement investigations because its warrant requirement does not apply to investigations that lack a law enforcement purpose. CAL. PENAL CODE § 1546.1(a) (West 2017); see also *infra* Section III.B (offering a detailed discussion of CalECPA's provisions).

10. CalECPA also protects electronic device information that goes beyond electronic communication information. See *infra* Section III.A.2.

11. § 1546.1(a).

by extending the warrant requirement to metadata, including location data. As one of the bill's sponsors explained, CalECPA "protects most electronic information, including personal messages, passwords and PIN numbers, geolocation data, photos, medical and financial information, contacts, social networking content, web browsing history, and metadata."¹²

Unlike analogous statutes, CalECPA requires a warrant for access to information about an electronic device that is not associated with a particular communication, including information that the device generates or that is merely stored on the device.¹³ Also unlike ECPA, CalECPA requires the government to furnish notice, in all cases, to the target of the investigation, and provides a suppression remedy for evidence gathered in violation of its terms. A suppression remedy significantly deters noncompliance by prohibiting the use of improperly obtained evidence in court.¹⁴

It is unsurprising that California would pioneer a comprehensive electronic communications privacy law, given the state's historic position at the vanguard of modern privacy regulators. But because CalECPA set out to do so much more to protect the privacy of electronic communications than ECPA and other analogous state laws, observers doubted the bill's prospects.¹⁵ In addition, CalECPA's suppression remedy necessitated that two-thirds or more of the legislature approve it. In fact, obtaining Governor Brown's signature loomed as the biggest hurdle to passage because the Governor had previously vetoed bills of more limited scope.¹⁶ In 2013, for example, the Governor had vetoed a bill that would have required a warrant and notice to the target when government entities compelled the disclosure of communications content

12. *Tech Industry Stands with Sen. Leno to Modernize Digital Privacy Protections*, ACLU OF N. CAL. (Feb. 9, 2015), www.aclunc.org/news/tech-industry-stands-sen-leno-modernize-digital-privacy-protections [<http://perma.cc/W8BP-SJYY>]. See *infra* Section V.A (discussing the ambiguity of the content of electronic communications).

13. CAL. PENAL CODE §§ 1546.1(a)(2), 1546(g).

14. CAL. PENAL CODE § 1546.4(a). See *infra* Section III.D.

15. This comment is based on the author's conversations with people involved with legislative reform efforts at the federal level.

16. S.B. 467, 2013-2014 Reg. Sess. (Cal. 2013) (vetoed Oct. 12, 2013); see also S.B. 1434, 2011-2012 Reg. Sess. (Cal. 2012) (vetoed Sep. 9, 2012). In his veto message for S.B. 467, Governor Brown complained that the bill's notice provision would go beyond federal law requirements. In vetoing S.B. 1434, which would have required a warrant for location data, Governor Brown remained unconvinced that the bill struck "the right balance between the operational needs of law enforcement and individual expectations of privacy." Letter from Edmund G. Brown, Jr., Governor of Cal., to Members of the Cal. State Assembly (Sept. 30, 2012), https://www.gov.ca.gov/docs/SB_1434_Veto_Message.pdf [<http://perma.cc/PQ5N-NPQB>].

from service providers. Unlike CalECPA, that bill omitted coverage of location data, metadata, or device-accessed data, and it lacked a suppression remedy.¹⁷

How did CalECPA, which was much more ambitious than such prior bills, then pass? A large coalition of technology companies, civil liberties and civil society groups, journalists, and academics spent over a year working hard to build a case for reform against a legal backdrop of existing state and federal law.¹⁸ Of course, timing also helped; CalECPA passed in a social context in which concern had built about law enforcement use of private data.

A. CALIFORNIA LAW

For years, California has positioned itself as an early adopter of privacy-protective legislation in the commercial context. For example, California was one of the first states to pass aggressive anti-spam legislation to protect users from privacy-invasion by unwanted communications¹⁹ and the first to pass a data breach notification law to protect consumers' data security.²⁰ California's requirement that online providers post their privacy policies in a conspicuous position has set the nationwide standard,²¹ and California has been quick to implement a version of the "right to be forgotten" for minors.²² In fact, a recently published book on California privacy law advised privacy compliance officers to plan to update their compliance policies regularly because "[t]he California legislature constantly enacts new laws."²³

But California has been much slower to modernize its rules for law enforcement access to electronic communication information. With the exception of the Reader Privacy Act of 2011, which requires a warrant-like court order before government agents may obtain customer records pertaining to book services,²⁴ those laws have not changed much in recent years. As

17. Cal. S.B. 467 § 5 (providing for a civil action of \$1,000).

18. See generally Dave Maas, *CalECPA and the Legacy of Digital Privacy: An Open Letter to Gov. Jerry Brown*, ELEC. FRONTIER FOUND. (Sept. 23, 2015), <https://www.eff.org/deeplinks/2015/09/open-letter-gov-jerry-brown-calcapa-and-legacy-technology> [<http://perma.cc/X37D-KF3Y>] (describing the extensive support for CalECPA).

19. CAL. BUS. & PROF. CODE § 17529–29.9 (West 2014).

20. CAL. CIV. CODE § 1798.82(a) (West 2017); see also *10 Years After S.B. 1368 California Attorney General Issues First Ever Report and Recommendations on Data Breaches*, INFOLAWGROUP LLP (July 1, 2013), <http://www.infolawgroup.com/2013/07/articles/breach-notice/10-years-after-sb-1386-california-attorney-general-issues-first-ever-report-and-recommendations-on-data-breaches/> [<http://perma.cc/N43F-UYQ9>].

21. California Online Privacy Protection Act, CAL. BUS. & PROF. CODE § 22575(a) (West 2014).

22. CAL. BUS. & PROF. CODE § 22580–81 (West 2015).

23. LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY § 3-12 (2016).

24. Reader Privacy Act, CAL. CIV. CODE § 1798.90 (West 2012).

previously mentioned, bills updating the laws to adapt to new electronic communications technologies have made it through the legislature, only to be vetoed by the Governor.²⁵

As a key backdrop, the California Constitution explicitly furnishes a right to privacy that restricts both private and public actors by conveying “inalienable rights,” including “pursuing and obtaining safety, happiness, and privacy.”²⁶ In addition, the California Supreme Court issued two opinions in the 1970’s that specifically rejected the United States Supreme Court’s “third-party doctrine,” under which the Court had found no reasonable expectation of privacy, and therefore no Fourth Amendment protection, in business records and telephone numbers dialed.²⁷ In contrast, the California Supreme Court held that people do not forfeit their reasonable expectations of privacy by using third parties to store their records.²⁸ California’s highest court determined that information sufficient to form a “virtual current biography” is subject to a reasonable expectation of privacy and California constitutional protection.²⁹ Because a list of telephone numbers could create such a virtual current biography,³⁰ the Court found a California constitutional right to privacy in an early form of metadata.³¹

Before California courts could apply those fundamental privacy protections to newly evolving communications technologies, California voters passed the Right to Truth in Evidence Initiative in 1984.³² This initiative amended the California Constitution to prohibit California courts from using

25. See *supra* notes 16–17.

26. CAL. CONST. art. I, § 1 (1982).

27. See *Smith v. Maryland*, 442 U.S. 735, 745–46 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976); see also generally Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007) (discussing the third-party doctrine); Stephen E. Henderson, *After United States v. Jones, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431 (2014) (same).

28. See *People v. Chapman*, 36 Cal. 3d 98, 109 (1984), *abrogated on other grounds by* *People v. Palmer*, 24 Cal. 4th 856 (2001) (requiring a search warrant for police access to a person’s name, phone number, and address when unlisted by a telephone company); *People v. Blair*, 25 Cal. 3d 640, 653–54 (1979) (protecting telephone numbers); *Burrows v. Superior Court*, 13 Cal. 3d 238, 243 (1974) (protecting bank records).

29. *Burrows*, 13 Cal. 3d at 247; see also *Blair*, 25 Cal. 3d at 652. The California Supreme Court in *Blair* did not require a warrant per se, but it reversed a denial of the defendant’s motion to suppress a log of telephone numbers and explained the need, under California law, for “a judicial determination that law enforcement officials were entitled thereto.” *Id.* at 655.

30. *Burrows*, 13 Cal. 3d at 247.

31. See *Blair*, 25 Cal. 3d at 652; see also *White v. Davis*, 13 Cal. 3d 757 (1975) (recognizing that government access to electronic communications, location data and metadata implicate rights of free expression and free association).

32. CAL. CONST. art. I, § 28(f)(2).

California law to grant suppression remedies to criminal defendants.³³ After 1984, a California judge could not grant a suppression remedy based on the California Constitution's protection of the telephone numbers dialed and disclosed by pen registers because the Fourth Amendment does not offer that protection.³⁴ Stated another way, since 1984 a California court may grant a suppression remedy based on California law only when the California legislature has passed, by at least a two-thirds majority, a new statute specifically permitting suppression.³⁵

Before CalECPA, California statutory law had little to say about California government entities obtaining access to electronic communication information from California corporations. Besides California's Wiretap Act,³⁶ and its Reader Privacy Act,³⁷ California's statutory scheme was incomplete and rather odd.³⁸ California statutory law required a warrant for law enforcement access to communications in a patchwork of scenarios.³⁹ For example, it required that California law enforcement agents obtain a warrant before obtaining information held by out-of-state companies and that out-of-state law enforcement agents obtain a warrant to obtain information from in-state companies.⁴⁰ Regarding in-state law enforcement demands for information from in-state companies, however, California statutes required a warrant only for information associated with a small subset of crimes in a narrow set of contexts.⁴¹ Promoters of CalECPA argued that, for much of the information

33. *Id.*

34. *See* 69 Ops. Cal. Att'y. Gen. 55, 55 (Cal. A.G. 1986) (opining that a search warrant could be used to authorize pen registers); 86 Ops. Cal. Att'y. Gen. 198, 198 (Cal. A.G. 2003) (clarifying that the federal pen register statute did not require adequate judicial review to authorize pen registers in California).

35. CAL. CONST. art. 1, § 28(f)(2).

36. CAL. PENAL CODE § 629.50 (West 2011); *see* Memorandum from the Cal. L. Revision Comm'n, State and Local Agency Access to Customer Information from Communication Service Providers: California Wiretap Statute and Related Law 8–17 (Oct. 1, 2014), www.clrc.ca.gov/pub/2014/MM14-50.pdf [<http://perma.cc/C8GY-4AAK>] [hereinafter CLRC MEMORANDUM 2014-50] (describing California's Wiretap Act, which closely parallels federal law).

37. *See* Reader Privacy Act, CAL. CIV. CODE § 1798.90 (West 2012).

38. CLRC MEMORANDUM 2014-50, *supra* note 36, at 18 (describing California's "fragmented statutory approach to government access to stored communications" and noting that it "has produced some odd inconsistencies").

39. *See id.* at 17–19.

40. CAL. PENAL CODE §§ 1524.2(b), 1524.3(a) (West 2017) (restricting affected companies to electronic communication services and remote computing services, as defined under federal law).

41. *See* CLRC MEMORANDUM 2014-50, *supra* note 36, at 18. The Commission discussed an identity theft statute requiring a warrant to request certain information associated with certain misdemeanor property crimes and certain crimes involving fraud or embezzlement,

CalECPA covers, Californians were left with a privacy right that lacked an effective enforcement remedy.⁴²

B. FEDERAL LAW

In the period preceding CalECPA's passage, federal law operated similarly to California law in that it promised, or at least suggested, rights without effective remedies. Just a few years before CalECPA's passage, however, the Supreme Court affirmed electronic communications privacy claims in two important cases that strengthened the case for CalECPA. The Court considered GPS tracking to be a Fourth Amendment search in *United States v. Jones*,⁴³ and recognized enhanced privacy interests in cell phone contents in *Riley v. California*.⁴⁴ Both decisions had rejected precedents decided before the advent of powerful new communications technologies as inapplicable in modern times.⁴⁵ In that way, the Supreme Court supported the need for specially-tailored legislation like CalECPA. The Sixth Circuit's *Warshak* decision further supported electronic communications privacy by requiring a warrant before law enforcement agents may compel service providers to disclose the emails they store.⁴⁶

At the same time, the Court has so constrained the availability of the suppression remedy in Fourth Amendment cases that many victims of unlawful searches have little incentive to challenge the constitutionality of warrantless practices. For example, the Sixth Circuit applied the Court's "good faith" doctrine to refuse to suppress more than 9,000 emails obtained without a warrant in violation of the *Warshak* defendant's Fourth Amendment rights.⁴⁷

but noted that "staff could not find any California statute governing a search warrant issued by a California court for service on a California corporation." *Id.*

42. See Shahid Buttar, *California Leads the Way in Digital Privacy*, ELEC. FRONTIER FOUND. (Oct. 21, 2015), <https://www.eff.org/deeplinks/2015/10/california-leads-way-digital-privacy> [<http://perma.cc/F8KV-SYH9>]; Nicole A. Ozer, *California Is Winning the Digital Privacy Fight*, TECHCRUNCH (Nov. 7, 2015), <http://techcrunch.com/2015/11/07/california-now-has-the-strongest-digital-privacy-law-in-the-us-heres-why-that-matters/> [<http://perma.cc/VRL6-Z8LT>].

43. 565 U.S. 400, 400 (2012) (finding long-term GPS tracking for an ordinary criminal investigation to be a Fourth Amendment search).

44. 134 S. Ct. 2473 (2014) (rejecting the search-incident-to-arrest exception to the warrant requirement for cell phone searches).

45. See, e.g., *Jones*, 565 U.S. at 408–09; *id.* at 430–31 (Alito, J., concurring); *Riley*, 134 S. Ct. at 2484–91.

46. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). Even outside of the Sixth Circuit, major providers like Facebook, Google, Microsoft and Yahoo! require a warrant for access to email contents on the basis of *Warshak*. See *Who Has Your Back? Government Data Requests 2016*, ELEC. FRONTIER FOUND., <https://www.eff.org/who-has-your-back-2016> [<http://perma.cc/9B5Z-2THA>] (last visited Mar. 23, 2018).

47. *Warshak*, 631 F.3d at 282.

Similarly, the district court, on remand, denied the *Jones* defendant's suppression remedy, using an expansive application of the good faith doctrine.⁴⁸ While the Court held in *Riley* that the search-incident-to-arrest exception to the warrant requirement does not apply to cell phone searches, the Court nonetheless affirmed that exigent circumstances may still excuse the lack of warrant.⁴⁹ Reports are that, despite *Riley*, at least some law enforcement agents seize phones incident-to-arrest without a warrant and use forensic devices to offload their contents, because they consider the arrest context consistently to present the risk of data loss—an exigent circumstance.⁵⁰ Moreover, the Supreme Court has not yet addressed Fourth Amendment regulation of other means of gaining access to cell phones or other devices, such as the increasing use of cell phone simulators, or StingRays.⁵¹

Prior to CalECPA, federal courts left location data, an area of great concern to CalECPA's proponents, ambiguously or completely unprotected.⁵² Federal appellate courts remain split on whether to require a warrant for location information stored with service providers. Most recent decisions have come out opposing such a requirement, although they have considered only a subset of location data and often assumed that it was not particularly revealing.⁵³ Meanwhile, the Supreme Court has indicated a concern for location

48. *United States v. Jones*, 908 F. Supp. 2d 203, 214–15 (D.D.C. 2012); Susan Freiwald, *The Davis Good Faith Rule and Getting Answers to the Questions Jones Left Open*, 14 N.C. J.L. & TECH. 341, 370 (2013). The Supreme Court's *Jones* decision, in fact, did not explicitly require a warrant or even probable cause for GPS tracking, which left the door open for arguments that the information could be acquired by satisfying a lower procedural hurdle like reasonable suspicion. *See id.* at 348–49.

49. *Riley*, 134 S. Ct. at 2494–95.

50. These reports are based on the author's conversations with those who have knowledge of law enforcement practices. Even though agents may not view the data until they obtain a warrant, the approach seems at odds with the Supreme Court's suggestion in *Riley* that placing a phone in a Faraday bag should suffice to protect against loss of data until a warrant may be obtained. *Id.* at 2487.

51. *See generally* Brian L. Owsley, *Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183 (2014); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134 (2013) (describing increasing use of StingRays in investigations).

52. The Supreme Court is considering the case of *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017), during the 2017 term. That case concerns whether the acquisition of historical cell site location data is a Fourth Amendment search and offers the Supreme Court the opportunity to clarify the question. The Sixth Circuit held that the compelled disclosure of that data from a provider is not a Fourth Amendment search. *Id.* at 887–90.

53. *See, e.g.*, *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (en banc) (finding no reasonable expectation of privacy in limited set of location-data records); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (same). *But see In re*

data privacy,⁵⁴ without addressing it directly, and federal district courts in California have required a warrant when law enforcement agents compel the disclosure of cell site location data from providers.⁵⁵ Federal courts have withheld protection entirely from other types of metadata, following the same interpretation of the third-party doctrine that led them to withhold protection from location data.⁵⁶ As previously described, California does not interpret its own Constitution as subscribing to the third-party doctrine.⁵⁷

As for federal statutory protection, CalECPA's proponents found ECPA to be outdated, incomplete, and ineffective.⁵⁸ As Part IV elaborates, ECPA requires a warrant for only a small subset of investigations and provides much weaker protections—or no protections at all—for the rest. Even when it does offer other protections, ECPA provides no suppression remedy, though it

Application of the U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3rd Cir. 2010) (rejecting application of the third-party doctrine to location data and leaving the statutory question of the need for a warrant open for magistrate judges to determine).

54. See, e.g., *Riley*, 134 S. Ct. at 2490 (“Historic location information is a standard feature on many smart phones and can reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building.”).

55. See, e.g., *United States v. Williams*, 161 F. Supp. 3d 846 (N.D. Cal. 2016) (granting motion to suppress cell site location information obtained using an improper warrant); *In re Application for Telephone Information Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) (rejecting application of the third-party doctrine and requiring a warrant for law enforcement access to historic location data); see also *United States v. Cooper*, No. 13-cr-00693-SI-1, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015) (following the Supreme Court’s reasoning in *Riley* and refusing to rely on outdated precedents to regulate newly intrusive investigative methods, but applying the good faith exception to deny suppression).

56. See, e.g., *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (finding no Fourth Amendment search when agents obtained “the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account”). But see *Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring) (expressing doubt about use of the third-party doctrine in modern communications context); *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013) (rejecting the application of traditional third-party doctrine to the NSA’s telephone metadata program).

57. See *supra* note 28 and accompanying text. The court in *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) required a warrant for access to historical location data and found reasonable expectations of privacy in the data based in part on the California Constitution. The court explained, “there is little doubt that the California Supreme Court’s holding [in *Blair*] applies with full force to the government’s application here, which seeks historical [location data] generated by a target cell phone’s every call, text, or data connection, in addition to any telephone numbers dialed or texted.” *Id.* at 1025. The court distinguished prior federal appellate decisions that found no warrant required for compelled location data. *Id.* at 1029.

58. See Jazdia Butler, *Eureka! More State “Laboratories of Democracy” Catalyze ECPA Reform*, CTR. FOR DEMOCRACY & TECH BLOG (Jan. 20, 2016), <https://cdt.org/blog/eureka-more-state-laboratories-of-democracy-catalyze-ecpa-reform/> [http://perma.cc/N7MR-QNAN]; Ozer, *supra* note 42.

does offer civil damages that CalECPA does not.⁵⁹ Importantly, ECPA generally dispenses with notice when stored communications are involved, which may leave victims of unlawful acquisition or interception of their stored electronic communications in the dark.⁶⁰ One large company recently brought a First Amendment challenge to ECPA's indefinite nondisclosure orders, arguing that they prevented the company from discussing how the government conducted its investigations of customers' data.⁶¹ Some bills to amend ECPA have gained traction, but they have merely clarified that the warrant requirement applies to the content of all electronic communications obtained from service providers.⁶² They have not expanded the warrant requirement to cover other types of data nor addressed ECPA's other deficiencies such as the lack of a notice requirement and a suppression remedy.⁶³

ECPA does set a floor upon which state statutes may enact more privacy-protective provisions.⁶⁴ Other states had already done so, though none in as comprehensive a fashion as CalECPA. For example, prior to CalECPA, several states had required a warrant for law enforcement access to all types of stored communications contents.⁶⁵ Several had required a warrant for law

59. 18 U.S.C. §§ 2707, 2708, 2712 (2012).

60. *See infra* Section IV.B.3 (explaining that notice is required only when content is acquired without a warrant, but not when a warrant is used or when non-content is acquired). Victims may learn of unlawful interceptions if they are charged with a crime, and the prosecutor discloses the evidence to them and reveals how it was obtained. *But see* Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177, 208–16 (2009) (describing the substantial number of investigations under ECPA that do not lead to criminal charges, thus no notice to targets).

61. *See* *Microsoft Corp. v. United States*, 233 F. Supp. 3d 887, 899–900 (W.D. Wash. 2017). The court denied the government's motion to dismiss because Microsoft had alleged facially valid First Amendment claims. *Id.* at 904–12.

62. *See* Email Privacy Act of 2017, H.R. 387, 115th Cong. (2017); Email Privacy Act of 2015, H.R. 699, 114th Cong. (2015).

63. *Id.*

64. *See* Memorandum from the Cal. Law Revision Comm'n, State and Local Agency Access to Customer Information from Communication Service Providers: Electronic Communications Privacy Act of 1986 at 44 (Aug. 21, 2014), <http://www.clrc.ca.gov/pub/2014/MM14-33.pdf> [<https://perma.cc/Y2CX-LBZP>] [hereinafter CLRC MEMORANDUM 2014-33] (reviewing legislative history and precedents and concluding that federal law “leaves room” for a statute like CalECPA); *see also* 18 U.S.C. § 2703(d) (2012) (“In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such state.”).

65. *See, e.g.*, TEX. CODE CRIM. PROC. ANN. art. 18.02, 18.20, 18.21 (West 2015) (requiring a warrant for electronic and wire communications content); MD. CODE ANN., CTS. & JUD. PROC. § 10-4A-04 (West 2014) (same).

enforcement access to stored location data,⁶⁶ and some had required a warrant for access to electronic device information.⁶⁷ As of CalECPA's passage, however, no other state statute covered as many categories as comprehensively.⁶⁸

C. CALECPA'S PASSAGE

CalECPA's proponents sought to bring clarity and uniformity to California law and to update it for the electronic age.⁶⁹ They argued that other states were leaving California behind by updating their laws to account for law enforcement acquisition of location data.⁷⁰ By increasing the types of information subject to judicial oversight, CalECPA would help ensure that law enforcement agents would not acquire, store, or potentially share more revealing electronic communication information than needed to investigate crimes and secure public safety. CalECPA would assure Californians that their use of essential modern technologies would be free from unjustified government surveillance.⁷¹ At the same time, CalECPA would provide for emergencies and other means to accommodate important government interests and also to spur innovation.

66. *See, e.g.*, ME. REV. STAT. tit. 16, § 648 (West 2017) (requiring a warrant for access to "location information of an electronic device"); N.H. REV. STAT. ANN. § 644-A:2 (2015) (same).

67. *See* UTAH CODE ANN. § 77-23c-102(1)(b) (West 2016) (requiring a warrant to "use, copy, obtain, or disclose . . . the location information, stored data, or transmitted data of an electronic device"); VA. CODE ANN. § 19.2-70.3(K) (2011) (requiring a warrant for law enforcement use of a "device to obtain electronic communications or collect real-time location data from an electronic device"). A few states have recently enacted laws requiring a warrant to use cell site simulator devices like StingRays. *See, e.g.*, Wash. Rev. Code Ann. § 9.73.270 (West 2016). In addition, the Justice Department under President Obama announced a new policy under which the devices may not be used without a warrant, and the information they collect must be limited. U.S. DEP'T OF JUSTICE, POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY (2015), <https://www.justice.gov/opa/file/767321/download> [<https://perma.cc/V3ZK-FS2T>].

68. Only two arguably require a warrant for metadata. *See* UTAH CODE ANN. §§ 77-23c-102(1)(a) (West 2016) (covering both location data and stored and transmitted data more generally); TEX. CODE CRIM. PROC. ANN. art. 18.21, § 4 (West 2015) (requiring a warrant for access to "electronic customer data" other than records that reveal a customer's identity or his use of the applicable service). Neither of those laws provides a suppression remedy.

69. *See* CAL. S. COMM. ON PUB. SAFETY, BILL ANALYSIS, S.B. 178, 2015–2016 Leg., Reg. Sess., at 7–8 (2015), http://spsf.senate.ca.gov/sites/spsf.senate.ca.gov/files/sb_178_analysis.pdf [<https://perma.cc/87G5-LLAS>]. S.B. 178 was the bill that became CalECPA.

70. *See* CAL. ASSEMB. COMM. ON PRIVACY & CONSUMER PROT., BILL ANALYSIS, S.B. 178, 2015–2016 Leg., Reg. Sess., at 4 (2015), http://www.leginfo.ca.gov/pub/15-16/bill/sen/sb_0151-0200/sb_178_cfa_20150619_152455_asm_comm.html [<https://perma.cc/UXS2-X9KP>].

71. *See id.* at 3–4.

A small group of privacy activists from the American Civil Liberties Union (ACLU) of Northern California and the Electronic Frontier Foundation (EFF) advised the bill's sponsors, Senators Leno and Anderson. As cosponsors, they assisted with the drafting of CalECPA, the preparation of support documents, and the coordination of the communications and lobbying efforts.⁷² Throughout the more than year-long process to make CalECPA a law, the sponsors and their advisors also received substantial support from a broad coalition of private and public enterprises.

CalECPA reflects its proponents' concern about the increase in law enforcement acquisition of electronic communications data for investigations.⁷³ In support letters, technology companies complained that current law was not providing enough certainty to build trust among their cloud customers.⁷⁴ Companies were likely especially interested in establishing the security of their customer data after the Snowden revelations about massive government surveillance for foreign intelligence purposes called that security into question.⁷⁵ Civil society organizations and journalists complained that the inadequate protection of electronic communication information

72. I was also a member of the small group of advisors on the bill's policy and language teams, as explained in the first footnote containing my author description. Staff members from the Center for Democracy and Technology also advised the bill's sponsors and the California Newspapers Associations was an additional official cosponsor.

73. See, e.g., *S.B. 178 Fact Sheet*, ACLU OF N. CAL. (Sept. 2, 2015), www.aclunc.org/sites/default/files/SB%20178%20CalECPA%20Fact%20Sheet_0.pdf [<https://perma.cc/8HF7-76FV>] (reporting that Google had experienced a 250% jump in government demands for information in "the last five years" and that AT&T experienced a 70% increase in government demands for location data in 2014—totaling more than 64,000 demands).

74. See *California's Electronic Communications Privacy Act – S.B. 178*, ELEC. FRONTIER FOUND. (Oct. 2015), <https://www EFF.org/cases/californias-electronic-communications-privacy-act-calecpa> [<http://perma.cc/3XFW-7TQL>] (posting support letters from sponsoring companies such as Adobe Inc., Airbnb, Apple, Dropbox, Facebook, Foursquare, Google, LinkedIn, Microsoft, Mozilla, Namecheap, Reddit, Snapchat and Twitter). Business organizations such as the California Chamber of Commerce, Small Business California, and the Internet Association also supported the bill. *Id.*

75. See Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 11:05 AM), <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> [<https://perma.cc/NR3V-CX3Z>]. See generally PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), https://www.pclob.gov/library/215-report_on_the_telephone_records_program.pdf [<https://perma.cc/CKD4-FEF3>] (discussing one of the programs that Mr. Snowden's disclosures made public); PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014), <https://www.pclob.gov/library/702-Report.pdf> [<https://perma.cc/M7KT-9558>] (discussing the other program).

chilled non-mainstream views and sources' speech.⁷⁶ Additionally, criminal defense organizations supported the bill's enhanced procedural protections.⁷⁷

Somewhat unexpectedly, given their previous opposition to similar, though more modest, bills,⁷⁸ several major law enforcement groups ended up withdrawing their opposition to CalECPA, notwithstanding its ambitious scope and aggressive terms.⁷⁹ Some involved in the legislative process credited the lack of law enforcement opposition as being a key factor in the Governor's decision to sign CalECPA into law.⁸⁰ Law enforcement groups, for their part, credited the sponsors' responsiveness to law enforcement concerns in explaining the withdrawal of their opposition.⁸¹ Over the course of several negotiated drafts of the bill, the sponsors made concessions to address law enforcement's needs.⁸² For example, the sponsors amended the bill's consent

76. See Mark Leno & Joel Anderson, *California Electronic Communications Privacy Act (CalECPA) – S.B. 178*, ACLU OF N. CAL. (May 2017), <https://www.aclunc.org/our-work/legislation/calecpa> [<https://perma.cc/T98L-MKGW>] (listing support from such organizations as Asian Americans Advancing Justice, Centro Legal de la Raza, Council on American-Islamic Relations and the National Center for Lesbian Rights).

77. *Id.* (listing support from such groups as: California Attorneys for Criminal Justice, California Public Defenders Association, and Citizens for Criminal Justice Reform). Groups supporting online civil liberties such as Tech Freedom, New America: Open Technology Institute, and the Internet Archive also supported the bill. *Id.*

78. The California Sheriffs', District Attorneys' and Police Chiefs' associations had all opposed the predecessor to CalECPA, S.B. 467. See CAL. S. RULES COMM., BILL ANALYSIS, S.B. 467, 2013–2014 Leg., Reg. Sess., at 4 (2013), www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0451-0500/sb_467_cfa_20130910_003407_sen_floor.html [<https://perma.cc/RM7D-KFXB>]. The California District Attorneys and Sheriffs had also opposed S.B. 1434. See CAL. S. RULES COMM., BILL ANALYSIS, S.B. 1434, 2011–2012 Leg., Reg. Sess., at 4 (2012), http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_1401-1450/sb_1434_cfa_20120525_10_2616_sen_floor.html [<https://perma.cc/XCH6-72J9>]; see also *supra* notes 16–17.

79. The California Sheriffs', District Attorneys' and Police Chiefs' associations all eventually came out as neutral on S.B. 178, with the San Diego Police Officers' Association even coming out in support. Several law enforcement groups withdrew their previous opposition to the bill over the course of negotiated amendments. Still, a few local law enforcement groups and the California Correctional Peace Officers Association remained opposed to the bill. See CAL. S. RULES COMM., BILL ANALYSIS, S.B. 178, 2015–2016 Leg., Reg. Sess. (2015), http://www.leginfo.ca.gov/pub/15-16/bill/sen/sb_0151-0200/sb_178_cfa_20150909_094155_sen_floor.html [<https://perma.cc/RGX3-NEZL>].

80. This is based on my conversations with coalition members.

81. See, e.g., Letter from Alan Wayne Barcelona, President, Cal. Statewide Law EnFt Ass'n., to Mark Leno, Senator, Cal. State Senate (Aug. 10, 2015), <https://www.eff.org/document/california-statewide-law-enforcement-association-removes-opposition-sb-178-calecpa> [<https://perma.cc/6X6A-EPGU>] (concluding that, after negotiations, CalECPA “is much closer to striking the appropriate balance between privacy concerns related to electronic communication, and the ability of law enforcement to effectively do its job keeping the public safe”).

82. See, e.g., CAL. PENAL CODE § 1546.1(c)(8) (West 2017) (permitting warrantless electronic device access in some correctional facilities in some circumstances). This section

provisions to facilitate online undercover investigations and added some specific exceptions to coverage during the legislative process.⁸³ But even with those concessions, as later Sections elaborate, CalECPA stands as an immensely privacy-protective statute.

CalECPA passed through the public safety committees with much legislative support.⁸⁴ The bill had to shed its detailed reporting requirements when it got to the Senate Appropriations Committee.⁸⁵ Those provisions would have facilitated study of the use and efficacy of new surveillance methods by requiring reports on the number and types of investigations conducted, the amount of information received, the number of users affected, the extent of information sharing, and other factors.⁸⁶ The committee determined that the record-keeping needed to permit government reporting would cost the state too much money.⁸⁷

The bill faced some opposition on the floor of the Assembly. Protect.org, an advocacy group dedicated to protecting children from harm, opposed the bill on the ground that it would inhibit online investigations of child pornographers and other child predators.⁸⁸ The group marshaled considerable late-breaking support from lawmakers, which jeopardized getting the two-

was added to the September 4, 2015 version of the bill after it was introduced. *See also id.* § 1546.1(g)(3) (permitting government entities to retain voluntarily disclosed information pertaining to child pornography). This section was added to the August 28, 2017 version of the bill after it was introduced.

83. *See infra* Section III.C.4; *see also Can Californians' Privacy Be Protected in a Wired World?*, L.A. TIMES (Sept. 3, 2015, 5:00 AM), <http://www.latimes.com/opinion/editorials/la-ed-privacy-20150903-story.html> [<https://perma.cc/WJ62-WM8X>] (opining that the opposition's "legitimate concerns appear to have been addressed by the earlier amendments").

84. S.B. 178 passed the Senate Public Safety Committee 6 to 1, and the Assembly Public Safety Committee 5 to 0 with 2 abstentions. *S.B. 178 Privacy: Electronic Communications: Search Warrant (2015–2016)*, CAL. LEGISLATIVE INFO., https://leginfo.legislature.ca.gov/faces/billVotesClient.xhtml?bill_id=201520160SB178 [<https://perma.cc/5GRD-SH4R>] (last visited Mar. 26, 2018).

85. *See* CAL. S. COMM. ON APPROPRIATIONS, BILL ANALYSIS, S.B. 178, 2015–2016 Leg., Reg. Sess., at 2–5 (2015), <https://www.eff.org/document/senate-appropriations-committee-sb-178-analysis> [<https://perma.cc/9WW3-2HZA>].

86. *See* S.B. 178, 2015–2016 Leg., Reg. Sess. § 1546.6 (Cal. 2015).

87. CAL. SENATE COMM. ON APPROPRIATIONS, *supra* note 85, at 5 (finding that the data collection and reporting activities required “could result in major one-time and ongoing costs, potentially in the tens of millions of dollars annually”).

88. *See PROTECT Analysis of S.B. 178, as Passed by the California Assembly, 9/8/15*, PROTECT (Sept. 9, 2015), <http://protect.org/178> [<https://perma.cc/XUE8-XZGJ>].

thirds votes needed.⁸⁹ CalECPA's proponents ultimately prevailed in the legislature.⁹⁰ One month later, the Governor signed the bill into law.⁹¹

III. CALECPA'S PROVISIONS

Under CalECPA, and subject to limited exceptions, government entities in California must obtain a circumscribed warrant before they may compel the disclosure of electronic communication information from service providers or obtain such information directly from electronic devices. CalECPA provides both mandatory and discretionary means for judges to confine warrants to relevant information, and it provides for the sealing or destruction of irrelevant information collected pursuant to those warrants. It requires notice to the target, even in emergencies and even when the targets may not be identified, although notice may be delayed in some cases. CalECPA permits a variety of challenges to investigations conducted under it and affords a suppression remedy to successful challengers. The following Sections discuss CalECPA's provisions in more detail.⁹²

A. WHO AND WHAT DATA IS PROTECTED?

1. *Who Is Protected?*

CalECPA protects those whose "service providers" hold their "electronic communication information."⁹³ Under CalECPA, "service provider" "means a person or entity offering an electronic communication service."⁹⁴ The statute defines an electronic communication service broadly to include "a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information."⁹⁵ Including those who merely act as intermediaries or store electronic communication information makes the

89. This is from the author's memory while working on the statute.

90. S.B. 178 passed the Senate by a vote of 34 to 4, with 2 abstentions, and passed the Assembly by a vote of 57 to 13 with 10 abstentions. CAL. LEGISLATIVE INFO., *supra* note 84.

91. *See* Zetter, *supra* note 2. In my view, the bill's opponents lost because they objected to the bill as a whole rather than offering tailored exceptions that would gut the bill. Because there was so much support for at least some reform, blanket opposition did not carry the day.

92. The organization of this Section generally follows that used by Lothar Determann in his book on California privacy law. *See generally* DETERMANN, *supra* note 23. I am indebted to him for his expertise and practical wisdom.

93. CAL. PENAL CODE § 1546.1(a)(1) (West 2017).

94. *Id.* § 1546(j).

95. *Id.* § 1546(e).

definition particularly broad.⁹⁶ CalECPA service providers thus include cloud storage services such as Dropbox, social media sites such as Facebook, and traditional email providers like Google (Gmail). While the expansiveness of CalECPA's coverage establishes that it should sweep more broadly than federal law by covering much more than traditional communication providers, the outer boundary of CalECPA's service provider category and hence its coverage, remains unclear.⁹⁷

CalECPA also protects those whose information is obtained directly from their devices rather than (or in addition to) from their service providers. CalECPA regulates law enforcement methods that target an electronic device, defined as "a device that stores, generates, or transmits information in electronic form."⁹⁸ CalECPA's device provisions are much more detailed than the few other device-access provisions that other states had previously passed.⁹⁹

2. *What Is Protected?*

CalECPA imposes its warrant scheme on government entities' access to two types of information: electronic communication information and electronic device information, collectively called "electronic information."

Electronic communication information includes "any information about an electronic communication or the use of an electronic communication service."¹⁰⁰ This definition encompasses electronic communications content information, associated metadata, and location data.¹⁰¹ It also explicitly includes IP addresses.¹⁰² CalECPA's use of technologically-neutral language makes it forward looking; any device can generate electronic communication information. Its broad terms will allow the category of information investigated to expand as techniques of identification grow, such as through

96. This definition can be compared to the analogous definitions of service provider under federal law, *see infra* notes 211–213, which do not include those who act as intermediaries or store information.

97. *See infra* Section V.A (discussing the ambiguity of CalECPA's definition of "service provider").

98. CAL. PENAL CODE § 1546.1(a)(2)–(3) (West 2017); *id.* § 1546(f).

99. *See* UTAH CODE ANN. § 77-23c-101 (West 2016); TEX. CODE CRIM. PROC. ANN. art. 18.21 (West 2015). Federal law lacks a device provision.

100. CalECPA defines an electronic communication as "the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system." CAL. PENAL CODE § 1546(c) (West 2017). CalECPA's definition closely tracks the federal version. 18 U.S.C. § 2510(12) (2012).

101. CAL. PENAL CODE § 1546(d) (West 2017).

102. *Id.* Section V.A also discusses the ambiguity of the content of electronic communications, particularly IP addresses.

biometrics. As mentioned, CalECPA subjects all the information included in this category, and the next, to the same tailored warrant requirement.

The second type of information CalECPA protects, electronic device information, includes information that a person has stored on their device as well as information that is generated through use of that device.¹⁰³ Presumably, much of what will be stored on a person's electronic device will be electronic communication information, but "electronic device information" may include more than electronic communication information. Individual photos, videos, and other information that may not be associated with a particular electronic communication would still be considered to be electronic device information when stored on a person's device. Similarly, information that a cell phone generates about its location does not have to be associated with a particular communication to be protected electronic device information.¹⁰⁴ Device identification numbers should also be included in this category.¹⁰⁵

3. *What Is Not Protected?*

CalECPA explicitly excludes "subscriber information" from the definition of electronic communication information; government entities do not need a CalECPA warrant to compel the disclosure of subscriber information from service providers.¹⁰⁶ CalECPA defines subscriber information as:

[T]he name, street address, telephone number, email address, or similar contact information provided by the subscriber to the service provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.¹⁰⁷

CalECPA explicitly preserves government entities' existing authority to use administrative, grand jury, trial, or civil discovery subpoenas to obtain subscriber information.¹⁰⁸

103. CAL. PENAL CODE § 1546(g) (West 2017).

104. *See also* Liebeskind, *supra* note 4 (suggesting that electronic device information includes information obtained from an IMSI catcher, or a cell site simulator device like a StingRay).

105. CAL. PENAL CODE § 1546(g) (West 2017) (including in "electronic device information" any information "stored on . . . an electronic device").

106. *Id.* § 1546(d).

107. *Id.* § 1546(j). *See infra* Section III.C.3 (comparing the information that may be obtained with a subpoena under CalECPA with that which may be obtained with a subpoena under ECPA).

108. CAL. PENAL CODE § 1546.1(i)(3) (West 2017).

CalECPA's exclusion of subscriber information from its warrant requirement reflects the understanding that such information does not change over time as do other types of electronic communication information. Because subscriber information is "static information," its acquisition by the government requires less judicial oversight than the acquisition of information that reveals someone's activities over a period of time.¹⁰⁹ Compared to the latter, static information is less likely to implicate intimate activities, or activities that reflect First Amendment values of speech and association. Further, as a practical matter, law enforcement agents need to have some investigative building blocks that they can obtain without having to establish probable cause. Subscriber information constitutes that type of building block that can establish probable cause for a warrant for access to more revealing and protected information.

B. WHO MUST COMPLY?

CalECPA casts a large net by imposing a warrant requirement on the acquisition of information by "government entit[ies]," which includes both state agencies and individuals within those agencies.¹¹⁰ By its terms, CalECPA regulates not just police, but everyone involved in the criminal justice system—from prosecutors to sheriffs to probation officers.¹¹¹ Its language also covers searches by public school and hospital officials and other government agency employees who use one of CalECPA's covered methods.

CalECPA's purposeful limitation significantly reduces the statute's reach, however. Notably, CalECPA does not impose its warrant requirement when a government entity compels the disclosure of electronic information for purposes other than "investigating or prosecuting a criminal offense."¹¹² In other words, outside of criminal investigations, when it comes to compelled disclosures, CalECPA permits the use of subpoenas to the extent permitted by

109. Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 163 (discussing static information).

110. CAL. PENAL CODE § 1546(i) (West 2017) (defining "[g]overnment entity" as "a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof").

111. *Id.*

112. *Id.* § 1546.1(b)(4) ("A government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device . . . [p]ursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense.").

other law.¹¹³ That means that a host of administrative inquiries and investigations will continue to proceed under subpoena regulations not specified in CalECPA.¹¹⁴ Though this limit is based on the purpose of the investigation and not on who conducts it, in practice it will reduce the type and number of government entities subject to CalECPA's warrant requirement.¹¹⁵

CalECPA's broad coverage led to numerous calls for exclusions. As passed, CalECPA contained only one categorical exclusion: it explicitly permitted prison officials to access electronic device information directly from devices seized in prisons, where it is illegal for inmates to have devices.¹¹⁶ The Governor signed into law a bill including some amendments to CalECPA in September of 2016.¹¹⁷ That bill made minor adjustments to the law and added additional carve-outs from coverage pertaining to probationers and parolees, and to the location information associated with "911" emergency calls.¹¹⁸

C. HOW TO COMPLY?

The following Subsections lay out the different investigative methods subject to CalECPA's warrant requirement and describe the circumscribed warrants CalECPA requires. The discussion then elaborates on those investigative methods that do not require a CalECPA warrant, either because they are explicitly excluded or because they involve voluntary disclosures, consent, or emergencies. Finally, the last Subsection describes CalECPA's comprehensive notice requirements.

1. Warrant-Regulated Methods

CalECPA effectively regulates by investigative method, rather than by the type of information acquired in an investigation.¹¹⁹ CalECPA subjects three different methods of accessing electronic information to the warrant

113. Use of the subpoena must not be prohibited by other federal or state law, and CalECPA disclaims any intent to expand any subpoena authority under state law. *Id.*

114. *See, e.g.*, CAL. GOV'T CODE §§ 11180, 11181(e) (West 2004).

115. Because CalECPA has incorporated subpoena access into its terms as a method of obtaining electronic information, however, such access will still be subject to CalECPA's remedies if done improperly. *See infra* Section III.D.

116. CAL. PENAL CODE § 1546.1(c)(8) (West 2017) (requiring that the device seized is not known or believed to be in "the possession of an authorized visitor" and that the seizure not otherwise be "prohibited by state or federal law").

117. S.B. 1121, 2015–2016 Leg., Reg. Sess. (Cal. 2016).

118. CAL. PENAL CODE § 1546.1(c)(9)–(11) (West 2017).

119. This follows the approach suggested by Professors David Gray and Danielle Citron. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71 (2013) ("Rather than asking *how much* information is gathered in a particular case, we argue here that Fourth Amendment interests . . . demand that we focus on *how* information is gathered.").

requirement; two involve compelled disclosure from third parties and the third involves direct interaction with an electronic device.

The first type of compelled disclosure that CalECPA subjects to its warrant requirement involves the compelled “production of or access to electronic communication information from a service provider.”¹²⁰ As mentioned above, government entities have increased their demands for information about customers’ electronic communications from service providers such as email providers and cell phone service providers. CalECPA imposes a warrant requirement on such demands and imposes a notice requirement as well.¹²¹

The second type of compelled disclosure occurs when a government entity compels the “production of or access to electronic device information from any person or entity other than the authorized possessor of the device.”¹²² Electronic device information includes information that a person has stored on their device as well as information that is generated through use of their device.¹²³ For example, CalECPA requires a California government entity to obtain a warrant before it may compel a device manufacturer that is not acting as a service provider (such as Apple), to divulge a device’s unique device ID (not electronic communication information) to facilitate cracking the device’s encryption.¹²⁴

The third investigative method that CalECPA imposes a warrant requirement upon is the direct interaction with an electronic device to gather electronic device information.¹²⁵ The warrant requirement applies when the government entity interacts with the device physically, such as by typing commands into a smart phone or computer to obtain information from that device. It also applies when the government entity uses electronic communications to obtain information from an electronic device, for example

120. CAL. PENAL CODE § 1546.1(a)(1) (West 2017).

121. *See infra* Section IV.C.6 (discussing notice provisions).

122. CAL. PENAL CODE § 1546.1(a)(2) (West 2017). *See also infra* notes 142–145 and accompanying text (discussing the justification for the authorized possessor carve out).

123. *See supra* Section III.A.2.

124. *Cf.* Katie Benner & Eric Litchtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html [<https://perma.cc/7JK8-UQE5>] (describing the standoff resulting from the FBI’s demand that Apple help unlock an encrypted iPhone); *In re Search of an Apple iPhone Seized During the Execution of Search Warrant on a Black Lexus IS300*, Cal. License Plate 35KGD20, No. ED 15-0451M, 2016 WL 618401, at *1–2 (C.D. Cal. Feb. 16, 2016) (ordering Apple to assist the FBI).

125. CAL. PENAL CODE § 1546.1(a)(3) (West 2017).

by using a StingRay to obtain information from a cell phone or by using a hacking-type method to obtain information from a computer.¹²⁶

2. Warrant Requirements

CalECPA generally prohibits the three investigative methods described in the immediately preceding Subsection, and then specifies the only way those methods may lawfully proceed. In the ordinary course, the investigative method will proceed by way of a CalECPA-specified warrant, to be described. But CalECPA also permits, when applicable, government entities to investigate pursuant to orders under California's Wiretap Act or Reader Privacy Act, both of which provide comparable protections to CalECPA.¹²⁷ After amendment in 2016, the law clearly permits access to electronic information by a Pen Register and Trap and Trace Order as well.¹²⁸ For simplicity, the rest of this Article will refer to CalECPA as requiring the warrant it specifies even though it also permits use of court orders under these three statutes instead.

When courts issue warrants under CalECPA, they follow CalECPA's additional requirements as well as the standard procedures for warrant applications set forth in California law.¹²⁹ The standard procedures require, among other things, that a search warrant be issued only upon a finding of probable cause, supported by an affidavit.¹³⁰ CalECPA specifically requires that the warrants it authorizes comply with all other provisions of California and federal law that impose additional requirements on the use of search warrants.¹³¹

CalECPA further limits the scope of information gathered pursuant to its authority to reduce the risk of unjustified information collection. While

126. *See generally* Pell & Soghoian, *supra* note 51; *see also* Letter from Richard Salgado, Google Inc., to the Judicial Conference Advisory Comm. on Criminal Rules 2 (Feb. 13, 2015), <https://assets.documentcloud.org/documents/1670588/13feb2015-google-inc-comments-on-the-proposed.pdf> [<https://perma.cc/E8KN-NBHH>] (describing various ways government entities have proposed obtaining "remote access" to devices).

127. CAL. PENAL CODE §§ 1546.1(b)(1)–(3), (c)(1)–(2) (West 2017); *see also* Reader Privacy Act, CAL. CIV. CODE § 1798.90 (West 2012).

128. CAL. PENAL CODE §§ 1546.1(b)(5), (c)(12) (West 2017) (permitting government entities to obtain electronic information from service providers and from electronic devices pursuant to pen register or trap and trace orders under California Penal Code section 638.50). The new provisions pertaining to pen register and trap and trace orders repeat several of the provisions in CalECPA, such as the requirements of sealing, notice, and the extensive remedies. *See id.* §§ 638.52, 638.54, 638.55.

129. *Id.* §§ 1546.1(b)(1), (c)(1) (describing the warrant as being "issued pursuant to Chapter 3" of the California Penal Code).

130. *Id.* § 1525.

131. *Id.* § 1546.1(d)(3).

background California law requires that the warrant particularly describe what is to be searched,¹³² CalECPA further requires that the warrant specify “the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought.”¹³³ By specifying additional parameters for its warrants, CalECPA endeavors to cut down on the “all accounts, for all time” orders that have become commonplace with digital searches.¹³⁴ Such searches can end up gathering so much information that they risk being fishing expeditions that violate the spirit, if not the letter, of the Fourth Amendment.¹³⁵

In a significant innovation, CalECPA further mandates that any information obtained that is “unrelated to the objective of the warrant” be sealed and unavailable without a further court order.¹³⁶ A court shall issue such an order only when federal or state law requires it, or when the court finds probable cause to believe the information is relevant to an active investigation.¹³⁷ This provision of CalECPA implements the data protection privacy principle that data collectors should specify the purposes for data collection, and precludes uses that are inconsistent with those purposes. It also maintains data quality by limiting the use of irrelevant data.¹³⁸ Data protection principles have, historically, found much more traction in Europe than in the United States.¹³⁹ CalECPA’s introduction of such principles into its law enforcement collection rules moves decidedly away from the notion that all digital information is available for law enforcement use.

132. *Id.* § 1525.

133. *Id.* § 1546.1(d)(1). This language was changed slightly in the 2016 amendment. See S.B. 1121, 2015–2016 Leg., Reg. Sess. (Cal. 2016).

134. *See, e.g.*, Brief of Erwin Chemerinsky et al. as Amici Curiae in Support of the Petition for a Writ of Certiorari at *2, *Rindfleisch v. Wisconsin*, 136 S. Ct. 128 (2015) (No. 14–1481), 2015 WL 4481305 (citing Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971 (2012)).

135. *See, e.g.*, *In re Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 6 (D.D.C. 2013) (rejecting the government’s overbroad request and issuing more limited search warrant to avoid granting a “general warrant” in violation of the Fourth Amendment’s particularity requirement).

136. CAL. PENAL CODE § 1546.1(d)(2) (West 2017).

137. *Id.*

138. *See* ORG. FOR ECON. COOPERATION & DEV., THIRTY YEARS AFTER THE OECD PRIVACY GUIDELINES at 21–22 (2011), <http://www.oecd.org/sti/ieconomy/49710223.pdf> [<https://perma.cc/8ZFFJ-5Q89>].

139. *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 122 (2017).

Besides requiring more specific warrant descriptions, CalECPA gives judges who issue warrants under it discretion to take other steps to reduce over collection. For example, CalECPA permits such judges to appoint a special master to ensure that only the information needed to achieve the warrant's objective is produced or accessed.¹⁴⁰ After the electronic information has been collected, a judge may, in response to a petition or on her own initiative, require the entity that has obtained the information to destroy any information “unrelated to the objective of the warrant.”¹⁴¹

3. *Exclusions from the Warrant Requirement*

CalECPA specifically excludes several methods of obtaining electronic information from its warrant requirement. First, CalECPA does not apply when government entities “compel the production of or access to electronic device information” from the device’s “authorized possessor”¹⁴²—either the device’s owner or someone the owner has authorized to possess the device.¹⁴³ That means agents may use a subpoena or another method to compel a person to disclose information stored on her own smart phone or computer, just as they may similarly compel the disclosure of that person’s private papers, diaries, photo albums, and the like.¹⁴⁴ Compulsion directed to a device’s authorized possessor falls outside CalECPA’s concern because such an order is served directly on the target; having notice, the target can exercise her right to contest the compelled disclosure on constitutional or other grounds.¹⁴⁵ In contrast, CalECPA regulates investigative techniques that may not—without its provisions—require notice to the person whose information is sought, and where the basis for challenge requires the clarification CalECPA provides.¹⁴⁶

140. CAL. PENAL CODE § 1546.1(e)(1) (West 2017); *see* Liebeskind, *supra* note 4 (noting that law enforcement sometimes refers to the special master as part of a “taint team”). The judge may decide to appoint a special master on her own or she may do so in response to a petition brought by the target or recipient of the order. CAL. PENAL CODE § 1546.1(e) (West 2017). Special masters are already provided for in § 1524(d), to which CalECPA refers.

141. CAL. PENAL CODE § 1546.1(e)(2) (West 2017). To avoid the destruction of exculpatory information, the destruction obligation does not kick in until the government entity has terminated the current investigation and related investigations. *See id.*

142. *Id.* § 1546.1(a)(2).

143. *Id.* § 1546(b).

144. *See, e.g.,* Mintz v. Mark Bartelstein & Assocs., 885 F. Supp. 2d 987, 994 (C.D. Cal. 2012).

145. Targets may raise constitutional (First Amendment, Fourth Amendment, Fifth Amendment, state Constitution) and any statutory claim in motions to quash. *See, e.g.,* Bellia & Freiwald, *supra* note 109, at 142 (describing two-step process); Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 806 (2005).

146. For example, the Fourth Amendment protection for location data is uncertain and is not yet established for other forms of metadata. Moreover, CalECPA establishes a

CalECPA requires notice and additional restrictions to protect the targets of investigations who are not as able to protect themselves as those who are directly served with orders for compelled disclosure.¹⁴⁷

Second, CalECPA permits government entities to use a variety of subpoenas to compel senders and recipients of communications to disclose their electronic communications.¹⁴⁸ The same logic applies to possessors of targeted electronic communications as applies to authorized possessors of targeted devices. Notice will be served directly on the person whose communications are sought and that person—particularly if she is the target of the investigation—can raise claims in response to the demand for disclosure.

Under CalECPA, the party who communicated with the investigation's target and whose communications with the target are disclosed by that target, has no privacy right violated by that disclosure. Presumably, that is based on application of the doctrine that the Fourth Amendment does not prevent a party to the communication from disclosing it to the government.¹⁴⁹ Patricia Bellia and I have argued that the law should distinguish between one's communication partner voluntarily disclosing one's communication, which is a risk one takes, and the government compelling the disclosure of that communication, which is a risk one should not be seen to assume merely by communicating.¹⁵⁰ By excluding from the warrant requirement electronic communication information that the government *compels* a person's communication partner to disclose, CalECPA accepts a broader application of the third-party doctrine than we recommended.¹⁵¹ CalECPA's provision opens the door not only to a target being compelled to disclose his communications partners' communications, but also to a target's communication partners being

comprehensive statutory suppression remedy for victims of unlawful seizure. *See infra* Section III.D.

147. Although the law of direct digital searches also lacks clarity, it is beyond CalECPA's scope. *See, e.g.*, Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005); Lily R. Robinton, *Courting Chaos: Conflicting Guidance from the Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311 (2010).

148. CAL. PENAL CODE § 1546.1(i)(1) (West 2017) (permitting subpoenas to “[r]equire an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication”).

149. *United States v. Charbonneau*, 979 F. Supp. 1177, 1184–85 (1997); *Hoffa v. United States*, 385 U.S. 293, 302 (1966).

150. Bellia & Freiwald, *supra* note 109, at 154.

151. CalECPA's approach does have support in the cases, however. *See id.* at 157; *see also* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 590 (2009) (arguing that agents may compel disclosure from third parties because witnesses can be compelled to testify about anything without Fourth Amendment oversight).

compelled to disclose the target's communications, without the protections of CalECPA or an opportunity for the target himself to raise claims.¹⁵²

In a related application of the third-party doctrine, CalECPA permits government entities to use a subpoena, rather than a warrant, to obtain electronic communication information from some employers. In particular, when an employer uses a company-provided email service, the company can be made to disclose, pursuant to a subpoena, information to which it has access.¹⁵³ Existing Fourth Amendment case law supports the idea that an employee has no right to privacy on her employer's server,¹⁵⁴ but a more privacy-protective approach would have recognized that employees should not have to forfeit their privacy just because they use a company email service, particularly as to their private messages.

4. *Voluntary Disclosures and Consent*

CalECPA entirely excludes from its coverage voluntary disclosures of electronic communication information by recipients of electronic communications.¹⁵⁵ To illustrate, if the subject of an investigation, Alice, sends an email to her friend Bob reporting on her intent to rob a bank, nothing prevents Bob from choosing to disclose to a government entity the contents of Alice's email or any other information about Alice's email that CalECPA would consider to be electronic communication information (including the time or date Bob received the email, Alice's IP address, etc.). The animating principle is that Alice, by communicating with Bob, has assumed the risk that Bob will disclose her communication and information about it to the government.¹⁵⁶

Service providers can also voluntarily disclose (1) electronic communication information, obviating the need for a warrant, and (2) subscriber information, obviating the need for whatever state law requires for

152. Notice to the target in situations where her communication partners are compelled to provide electronic communication information would have helped with this problem. Early drafts of CalECPA had broader notice provisions.

153. CAL. PENAL CODE § 1546.1(i)(2) (West 2017) (permitting a government entity to “[r]equire an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity”).

154. *See, e.g.,* United States v. Simons, 206 F.3d 392, 401–02 (4th Cir. 2000); Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979 (2011).

155. CAL. PENAL CODE § 1546.1(a)(3) (West 2017).

156. *See supra* notes 149–152 and accompanying text.

compelled disclosure—presumably a subpoena.¹⁵⁷ CalECPA places two significant limits on these voluntary disclosures. First, they must not otherwise be prohibited by state or federal law.¹⁵⁸ Because ECPA constrains when service providers (as it defines them) may disclose some electronic communication information, CalECPA incorporates those limits.¹⁵⁹ For example, ECPA permits service providers to disclose such information to government entities only with the user’s consent, as necessary to render service or to protect the provider’s rights or property, and in emergencies.¹⁶⁰

Second, the government must destroy, within ninety days, any electronic communication information it receives pursuant to voluntary disclosure unless it first (1) obtains the consent of the sender or recipient, (2) obtains a court order, or (3) reasonably believes the information relates to child pornography.¹⁶¹ These limits on retention of voluntarily-disclosed information significantly constrain the government’s ability to exploit voluntary disclosures as end runs around CalECPA’s warrant requirements.

Government entities can attain direct access to an electronic device without obtaining a warrant when they get the specific consent of the authorized possessor of the device.¹⁶² The authorized possessor’s “specific consent” must be “provided directly to the government entity seeking information,” which should rule out government entities’ reliance on terms of service—to which the government entity is not a party—to establish consent to search.¹⁶³ Specific consent does not require knowledge that one is giving consent to a government entity, so it can be given unwittingly to an

157. CAL. PENAL CODE § 1546.1(f) (West 2017).

158. *Id.*

159. *See* 18 U.S.C. § 2702 (2012). Federal preemption would require that CalECPA not permit disclosure of information when federal law would prohibit it, since ECPA sets a floor on electronic communications privacy protection that the states may not go below. *See supra* note 64 and accompanying text.

160. 18 U.S.C. §§ 2702(b)(3), (c)(2) (2012). A service provider may also disclose contents information to a law enforcement agency if they obtain it inadvertently and it appears to relate to the commission of a crime. *Id.* § 2702(b)(7).

161. CAL. PENAL CODE § 1546.1(g) (West 2017). Before granting an order, the court must ensure either that “the conditions justifying the initial voluntary disclosure persist . . . or there is probable cause to believe that the information constitutes evidence that a crime has been committed.” *Id.*

162. *Id.* § 1546.1(c)(3). When the government entity believes in good faith that a device is lost, stolen or abandoned, CalECPA permits that entity to access electronic device information on the device solely to “attempt to identify, verify, or contact the owner or authorized possessor of the device.” *Id.* § 1546.1(c)(6). The owner of a device can also give specific consent to search it when the device has been reported lost or stolen. *Id.* § 1546.1(c)(4).

163. *Id.* § 1546(k).

unidentified undercover agent.¹⁶⁴ In addition, one specifically consents to the receipt of an electronic communication by members of the intended audience of that communication, which includes members of a listserv or chat room.¹⁶⁵ This provision facilitates undercover operations such as when an unidentified agent receives evidence of a crime as part of a larger audience.

5. *Emergency Provisions*

CalECPA does not specifically provide for compelled disclosure orders in emergencies, but service providers can use their good-faith belief that an emergency exists to justify their voluntary disclosure of electronic communication information under federal ECPA.¹⁶⁶ As described above, CalECPA explicitly incorporates ECPA's voluntary disclosure provisions so that such disclosures are not subject to CalECPA's warrant requirement.

CalECPA does contain its own emergency provision for direct access to electronic devices. This provision permits such access without a warrant or other order when a "government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person" requires electronic device information access.¹⁶⁷ CalECPA limits recourse to this provision by using language associated with serious emergencies.¹⁶⁸ Further, within three days of obtaining the information, the government entity must establish before a court sufficient factual support for the claimed emergency.¹⁶⁹ Alternatively, the government entity can file an application for a warrant under CalECPA.¹⁷⁰ If the court does not grant a warrant or approve the emergency disclosures, then the court must order the immediate destruction of all information obtained and provide, if it has not done so already, immediate notice to the target of the disclosure.¹⁷¹

6. *Notice Requirements*

Under CalECPA, the government entity who obtains information via a warrant or an emergency order must furnish notice to the identified targets.¹⁷² Notice must be furnished contemporaneously with the warrant's execution,

164. *Id.*

165. *See id.*

166. 18 U.S.C. § 2702(b)(8) (2012).

167. CAL. PENAL CODE § 1546.1(c)(6) (West 2017) (tracking ECPA's emergency provision language).

168. *Id.* § 1546.1(h).

169. *Id.*

170. *Id.*

171. *Id.*

172. *Id.* § 1546.2(a). Notice may be served by first class mail, email, or other reasonably effective means.

or, in the case of an emergency, within three days of receiving the information.¹⁷³ CalECPA requires that the notice include a copy of the warrant and the nature of the compelled or requested information.¹⁷⁴

Government entities may request from the court a time extension for providing notice and an order prohibiting any party providing information from notifying the target that information has been sought.¹⁷⁵ The court may grant such orders when it finds reason to believe that notifying the target may have an adverse result; however, the order only lasts as long as the adverse result would exist, or up to ninety days, when the order becomes renewable.¹⁷⁶ When the government entity eventually does give notice, CalECPA requires it to furnish to the target a statement of the grounds for the court's determination to grant the delay, along with the information ordinarily required for notice.¹⁷⁷ Additionally, with delayed notice, the government entity must later provide to the target either a copy of all of the electronic information obtained or a summary of that information, including the number and type of records disclosed and the time period covered by such records.¹⁷⁸ These additional requirements serve as a burden on the request to delay notice.

As an interesting innovation, CalECPA requires the same information (basic notice information and additional information in cases of delayed notice) to be provided to the California Department of Justice (CaDOJ) in cases when the target may not be identified.¹⁷⁹ The CaDOJ must publish reports it derives from such information on its website within ninety days of receiving the information.¹⁸⁰ This mechanism provides transparency in investigations such as cell tower dumps and others that involve the collection

173. *Id.*

174. Notice must also state the government investigation under which the information is sought with reasonable specificity. *Id.* For emergency disclosures not involving warrants, the government entity must include a written statement that describes the facts that gave rise to the emergency. *Id.*

175. *Id.* § 1546.2(b)(1). While CalECPA does permit the government entity to request gag orders, it provides no other limitation on any party's ability to disclose information about requests for information. *Id.* § 1546.2(d).

176. *Id.* §§ 1546.2(b)(1)–(2), 1546(a) (defining an “adverse result” to match 18 U.S.C. § 2705(a)(2)). *See* Smith, *supra* note 60 (discussing the problem with indefinite gag orders and delays of notice in the federal system).

177. *Id.* § 1546.2(b)(3).

178. *Id.*

179. *Id.* § 1546.2(c).

180. *Electronic Search Warrant Notifications*, CAL. DEPT OF JUSTICE, <https://openjustice.doj.ca.gov/data> [<https://perma.cc/5GRU-XVHH>] (last visited Mar. 27, 2018). It may redact names, presumably of investigators, and other personal identifying information from the reports.

of information from unidentified targets.¹⁸¹ That should facilitate the ability of interested parties to monitor the CaDOJ's website for problematic patterns and practices.¹⁸²

D. SANCTIONS AND REMEDIES

CalECPA also provides a statutory suppression remedy. Under its terms, “any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of [CalECPA].”¹⁸³ The new law incorporates procedures already in place under California law for handling suppression motions.¹⁸⁴ California courts have interpreted these provisions not to apply when law enforcement agents violate the pertinent statutes in merely technical ways.¹⁸⁵ But the state procedures do not incorporate the expansive exceptions that courts have used to deny suppression remedies in Fourth Amendment cases under the doctrine of good faith.¹⁸⁶ The real risk that evidence collected will be excluded at trial furnishes government entities with significant incentives to comply with CalECPA's rules on obtaining and retaining information, as the suppression provision explicitly refers to both.

In addition to suppressing unlawfully obtained information, CalECPA permits individuals, service providers, and others involved in investigations to petition the issuing courts to “order the destruction of any information obtained in violation of [CalECPA], or the California Constitution, or the

181. *See, e.g., In re Application for Cell Tower Records Under 18 U.S.C. § 2703(d)*, 90 F. Supp. 3d 673, 674–77 (S.D. Tex. 2015) (granting an order that compelled seven cell phone service provider to disclose data from cell towers serving a crime scene during the ten minute period that the crime transpired); Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1 (2013) (arguing that cell tower dumps implicate reasonable expectations of privacy and are not covered by the Stored Communications Act).

182. Unfortunately, reporting provisions present in the early versions of CalECPA that would have furnished even greater transparency had to be dropped during the legislative process because of the expense of compliance. *See supra* notes 85–87 and accompanying text. The New York and New Mexico bills cited above, *supra* note 5, both would require extensive annual reporting of the kind that CalECPA had to drop.

183. CAL. PENAL CODE § 1546.4(a) (West 2016).

184. *Id.* (referring to the procedures in California Penal Code section 1538.5(b)–(q)).

185. *See, e.g., People v. Hoag*, 83 Cal. App. 4th 1198 (Cal. Ct. App. 2000).

186. *See, e.g., United States v. Leon*, 466 U.S. 897, 922 (1985). *See generally* TRACEY MACLIN, *THE SUPREME COURT AND THE FOURTH AMENDMENT'S EXCLUSIONARY RULE* (2013) (describing the origin and gradual erosion of the exclusionary rule).

United States Constitution.”¹⁸⁷ Petitioners may also ask the court to void or modify a warrant, order, or other legal process that violates CalECPA.¹⁸⁸

CalECPA authorizes the Attorney General to bring a civil action to compel any government entity to comply with its terms.¹⁸⁹ The statute does not provide for fines or other damage awards for victims of unlawful investigations. Its terms do not authorize private actions against entities who improperly furnish information to investigators or otherwise assist them. In fact, CalECPA immunizes corporations and their agents from any cause of action for complying with any process issued pursuant to the chapter.¹⁹⁰ Affording such immunity certainly removes one way of deterring noncompliance with CalECPA, but it may have been essential to obtaining the enthusiastic participation of private companies in the CalECPA coalition.¹⁹¹

IV. WHAT SETS CALECPA APART FROM FEDERAL LAW

Compared to ECPA, CalECPA requires warrants for more investigations; its warrants impose more restrictive requirements; it provides more notice to targets; and it furnishes more significant remedies. Congress has shown significant support for, but has not yet passed, ECPA reform bills that would move ECPA closer to CalECPA by expanding its warrant requirement to cover the compelled disclosure of all electronic communications content acquired from service providers (as ECPA defines them).¹⁹² But those bills do not close any of the other significant gaps between ECPA and CalECPA nor do they adopt any of CalECPA’s other innovative features. Regardless of the proposed reforms, CalECPA still stands head and shoulders above federal law in protecting the privacy of modern communications.

The following provides more detail on the differences between ECPA and CalECPA. The discussion will briefly cover differences between California’s Wiretap and Pen Register Acts and their federal analogs before focusing on the differences between CalECPA and the federal Stored Communications Act (“SCA”), which is the second of ECPA’s three titles.¹⁹³

187. CAL. PENAL CODE § 1546.4(c) (West 2016).

188. *Id.*

189. *Id.* § 1546.4(b).

190. *Id.* § 1546.4(d).

191. *See infra* Section V.A (discussing the uncertainty about whether companies are truly immune from liability).

192. *See* Email Privacy Act of 2017, H.R. 387, 115th Cong. (2017); Email Privacy Act of 2015, H.R. 699, 114th Cong. (2015).

193. Stored Wire and Electronic Communications and Transactional Records Access, Pub. L. No. 99–508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 USC §§ 2701–09,

A. CALECPA VERSUS FEDERAL WIRETAP AND PEN REGISTER LAW

1. *Wiretap Law Differences*

The California Wiretap Act is modeled after federal law.¹⁹⁴ A significant difference is that CalECPA makes suppression and other remedies available to victims of improper interceptions of electronic communications, while the federal provisions specifically deny suppression as a remedy for improper investigations of electronic communications.¹⁹⁵

2. *Pen Register Law Differences*

Pen registers obtain metadata, such as telephone numbers dialed and addressing information, in real time.¹⁹⁶ Prior to CalECPA, California lacked a specific Pen Register Act.¹⁹⁷ After passage of CalECPA and an amendment to it to reconcile a pen register law that was passed the same year,¹⁹⁸ pen register orders are generally subject to all of CalECPA's requirements and protections, described above, with a few minor modifications.¹⁹⁹ ECPA, by contrast, requires only a rubber-stamp court order based on relevance for investigations that obtain dialing, routing, addressing, and signaling (DRAS) information in

2711–12). ECPA's provisions covering interceptions, or wiretaps, make up its first title and its pen register provisions are located in its third title.

194. CLRC MEMORANDUM 2014-50, *supra* note 36, at 8–17. Note that outside the law enforcement context, California requires two parties to consent for wiretapping to be valid, while federal law requires only one party to consent. *Id.* at 4 (describing other exceptions available under federal law that California law does not recognize).

195. *See* 18 U.S.C. § 2515 (2012) (providing a statutory suppression remedy only for improper interceptions of wire and oral communications). Note that California's Wiretap Act has its own more limited suppression remedy as well as a provision for civil damages subject to good faith reliance. CLRC MEMORANDUM 2014-50, *supra* note 36, at 15–17.

196. *See* Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1295 (2005); Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 982–89 (1996).

197. CLRC MEMORANDUM 2014-50, *supra* note 36, at 19 (noting that pursuant to an opinion of the Attorney General, California law enforcement could use search warrants to authorize pen register and trap and trace investigations).

198. A.B. 929, covering pen registers and trap and trace devices, passed just before CalECPA, which created confusion as to which governed. Assemb. B. 929, 2014–2015 Leg., Reg. Sess. (Cal. 2015). S.B. 1121 and A.B. 1924 passed the next year and reconciled the two laws. *See* S.B. 1121, 2015–2016 Leg., Reg. Sess. (Cal. 2016). The new provisions require that the magistrate find “the information likely to be obtained . . . is relevant to an ongoing investigation and that there is probable cause to believe that the pen register or trap and trace device will lead to” certain types of evidence. CAL. PENAL CODE § 638.52(b) (West 2016).

199. For example, the pen register provisions permit investigations to last for sixty days, with extensions, and for information to be periodically furnished to the supervising officer. CAL. PENAL CODE §§ 638.52(e), (f), (j) (West 2016). Standard search warrants a void after ten days under California Penal Code § 1534(a).

real-time.²⁰⁰ ECPA's pen register provisions do not provide for notice to targets but rather provide for automatic sealing of orders and gag orders on providers who install pen registers.²⁰¹ ECPA provides no remedies for improper pen register installations, which means no statutory suppression remedy nor even a right to recourse through civil actions exists.²⁰²

B. CALECPA COMPARED TO THE STORED COMMUNICATIONS ACT (SCA)

1. *Who Is Protected?*

Like CalECPA, the SCA protects the privacy of those whose electronic communication information is stored with third-party service providers. Unlike CalECPA, however, the SCA does not protect information stored on electronic devices.²⁰³ That leaves law enforcement access to device-stored data—where not regulated by state laws like CalECPA—covered only by the Supreme Court's decision in *Riley v. California*.²⁰⁴ As discussed in Section II.B, *Riley* applies in the limited context of searches incident-to-arrest; in that context, its exception for exigent circumstances may leave many cell phones and other devices vulnerable to warrantless searches.²⁰⁵ Outside of the search-incident-to-arrest context, searches conducted solely pursuant to Fourth Amendment law face much uncertainty as to when notice is required, how to particularize the warrant, what remedy is available, and other questions to which CalECPA provides much clearer guidance.

2. *What Is Protected and How to Comply*

The greatest difference between the SCA and CalECPA lies in their scope. The SCA imposes a warrant requirement on access to only a subset of

200. 18 U.S.C. §§ 3121, 3123 (2012). JAMES CARR & PATRICIA BELLIA, *THE LAW OF ELECTRONIC SURVEILLANCE* 4:84 (2014) (explaining that the Pen Register Act does not contemplate independent judicial review of orders).

201. 18 U.S.C. § 3123(d) (2012).

202. In theory, the knowingly improper installation or use of a pen register could incur criminal liability. *See* 18 U.S.C. § 3121(d) (2012). It also violates the SCA for a government entity to willfully disclose pen register obtained information outside of official duties. *See id.* § 2707(g). *See* CLRC MEMORANDUM 2014-33, *supra* note 64, at 35.

203. 18 U.S.C. § 2702 (2012).

204. 134 S. Ct. 2473 (2014).

205. *See supra* notes 49–51 and accompanying text (discussing the differences between *Riley* and CalECPA). Note also that while *Riley* would permit access for exigent circumstances, the comparable CalECPA emergency provision would excuse the need for a warrant only when there is a good faith belief that danger of death or serious physical injury require access. CAL. PENAL CODE § 1546.1(c)(5) (West 2017).

electronic communications contents,²⁰⁶ and does not require a warrant for law enforcement access to some contents or to any metadata, including location data.²⁰⁷ In particular, the SCA requires a warrant only to compel the disclosure of the contents of electronic communications that have been in electronic storage for 180 days or less on an electronic communications service.²⁰⁸ Counter-intuitively, because they are likely to be more important to the user, electronic communications contents, like emails, stored more than 180 days are subject to a procedural hurdle that is easier to satisfy than probable cause.²⁰⁹

In contrast, CalECPA's uniform warrant requirement is surely its most privacy-protective feature. CalECPA applies its warrant requirement to the broad category of electronic information, which includes contents, metadata, location data, and electronic device data. Also unlike the SCA, CalECPA uses a broader definition of service providers, to include those who act as mere intermediaries in the transfer of electronic communications as well as those who merely store them.²¹⁰ CalECPA's broad definition of service provider should yield many more covered entities than the comparable federal language and much more covered information.

The SCA defines its service providers, which must be either an "electronic communications service"²¹¹ (ECS) or a "remote computing service"²¹² (RCS) in ways that further limit the scope of the SCA's warrant protection.²¹³ For example, based on those statutory definitions and the definition of "electronic

206. *See* 18 U.S.C. § 2510(8) (2012) (defining "contents" as "any information concerning the substance, purport, or meaning of that communication").

207. *Id.* §§ 2703(a), (b)(1)(A).

208. *Id.* § 2703(a).

209. The SCA defines electronic communications similarly to CalECPA. The SCA treats electronic communications and wire communications the same, but lists them separately. 18 U.S.C. §§ 2510(1), (12) (2012). In contrast, CalECPA includes communications sent by wire in its definition of electronic communications, thereby treating wire communications as a subset of electronic communications. CAL. PENAL CODE §1546(c) (West 2017).

210. The SCA also limits RCS's to those who provide services to the public. 18 U.S.C. § 2711(2) (2012).

211. *Id.* § 2510(15) ("[E]lectronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications.>").

212. *Id.* § 2711(2) (defining "remote computing service" to mean "the provision to the public of computer storage or processing services by means of an electronic communications system").

213. CLRC MEMORANDUM 2014-33, *supra* note 64. The SCA covers communications contents held by RCS's as opposed to ECS's only when those communications are held or maintained "on behalf of, and received by means of electronic transmission from . . . a subscriber or customer of such remote computing service" and held or maintained "solely for the purpose of providing storage or computer processing services to such subscriber or customer," with the RCS not being able to access the contents of the communication for any other purpose. 18 U.S.C. § 2703(b)(2) (2012).

storage,”²¹⁴ the federal Department of Justice (DOJ) has taken the position that emails that have been opened, accessed, or downloaded are not protected by SCA’s warrant requirement. The DOJ has opined that such emails stored by providers that do not offer service to the public, like universities, the government, and corporations, fall entirely outside the protections of the SCA.²¹⁵ Since 2013, DOJ policy has been to require a warrant for access to the content of all emails, despite the terms of the statute, but that practice could change outside of the Sixth Circuit, where the *Warshak* case governs.²¹⁶

As another example, a California district court found the social networking site LinkedIn to qualify as neither an ECS nor an RCS with respect to its customers’ web browsing information that it shared with third parties. The court therefore denied plaintiffs’ claims arising under the SCA.²¹⁷ CalECPA’s broad definition of service provider would surely have covered LinkedIn and the browsing information that it shared.²¹⁸

Even when the SCA does require a warrant requirement for law enforcement access, the federal statute does not require that the warrants issued under it be as tailored as CalECPA’s warrant are in order to avoid excessive information collection. Service providers responding to SCA warrants may be compelled to disclose everything they have about a target. In *Warshak*, for example, the service provider disclosed thousands of emails from Warshak’s account, spanning the nine years that he held his account with that provider.²¹⁹ The SCA also lacks any mechanisms for the segregation or deletion of irrelevant data.

The SCA, unlike CalECPA, provides a graduated and complex set of hurdles to obtaining different types of communications depending on their characteristics. Regarding communication contents, if they are held in

214. 18 U.S.C. § 2510(17) (defining “electronic storage” to include “temporary, intermediate storage . . . incidental to the electronic transmission” and storage “for purposes of backup protection” of the communication by an electronic communication service.”).

215. U.S. DEP’T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 123–26, 138 (3d ed. 2009), www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [<https://perma.cc/LX89-BKDA>] [hereinafter DOJ Manual]. See 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, 1215–18 (2004).

216. H.R. REP. NO. 114–528, at 9 (2014). The Ninth Circuit has also used a broader definition of electronic storage that does not support the DOJ’s former interpretation. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1076–77 (9th Cir. 2004).

217. *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1022–24 (N.D. Cal. 2012).

218. See ACLU OF N. CAL., *supra* note 12 (describing various types of information covered by CalECPA, including social network content and web browsing data).

219. See *Bellia & Freiwald*, *supra* note 109, at 130 (discussing the federal case against Warshak).

electronic storage by an RCS or held for more than 180 days by an ECS, government entities may acquire them with a subpoena if they give notice, or they may obtain a court order (“D order”)²²⁰ after meeting a procedural hurdle between the mere relevance standard and probable cause.²²¹ The D order is available only when the information sought is “relevant and material to an ongoing criminal investigation.”²²²

Under the SCA, information that is not the contents of a communication falls into one of two categories: it is either a “record or other information pertaining to a subscriber to or customer of” an ECS or an RCS, or it is outside the SCA’s scope.²²³ Thus, electronic device data that is stored on personal devices rather than by an SCA service provider would be protected by CalECPA’s warrant requirement but not protected by the SCA.

Whether the SCA even includes location data within its scope is unclear, which is not that surprising considering that the SCA was drafted in 1986, well before cell phones were in popular use. Most judicial opinions on the topic have assumed that the SCA’s records provision includes data collected by cell phone service providers that indicate which cell towers cell phones use when they make and receive calls.²²⁴ But some judicial opinions have found location data to be generated by a “tracking device”—a cell phone—and therefore excluded from SCA coverage.²²⁵ If the SCA’s records category includes location data, then agents may compel covered providers to disclose the data when they get a D order. It is unclear what rule applies if location data falls outside of the SCA’s coverage.²²⁶ The Fourth Amendment’s treatment of

220. It is called a D order because it is obtained under procedures detailed in 18 U.S.C. § 2703(d).

221. 18 U.S.C. § 2703(b) (2012). A D order requires “specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought [is] relevant and material to an ongoing criminal investigation.” *Id.* § 2703(d). Reformers have pressed for legislation to mandate a uniform warrant standard for access to all communications content. *See supra* note 192 and accompanying text.

222. § 2703(d). The limit on D orders indicates that the SCA, like CalECPA, is intended to regulate law enforcement investigations, although, like CalECPA, its terms refer generally to government entities. *See supra* notes 112–114 and accompanying text (describing how CalECPA leaves California law as it found it regarding investigations that do not have a law enforcement purpose).

223. 18 U.S.C. § 2703(c) (2012); *see also infra* Section V.A (elaborating on how the SCA defines service provider).

224. *See, e.g.,* United States v. Graham, 824 F.3d 421, 428 (4th Cir. 2016) (en banc).

225. *See* Susan Freiwald, *Light in the Darkness: How the LEATPR Standards Guide Legislatures in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 875, 883–86 (2014) (describing courts’ analyses and explaining that ECPA’s definition of electronic communications excludes information generated by a tracking device.)

226. *Id.*

location data remains uncertain; many, but not all, cases have found no warrant required for access to historical location data.²²⁷

CalECPA imposes its warrant requirement on location data, broadly defined, stored with a service provider because it includes the “location of the sender or recipients at any point during the communication” in the definition of electronic communication information.²²⁸ By bringing location data, however collected, so clearly within the scope of the warrant requirement, CalECPA brings helpful clarity to what has been a particularly muddled area of the law. It also protects information about people’s movements, which several scholars and courts have agreed should receive the judicial oversight that a warrant procedure entails.²²⁹

The SCA does not treat all “records” as subject to the D order; some of them are available pursuant to a subpoena—mirroring much of the information that CalECPA permits access to with a subpoena in its “subscriber information” category.²³⁰ The SCA permits access to much more information with a subpoena than CalECPA does, however. In particular, the SCA permits government entities to obtain call data records and subscriber numbers or identities with a subpoena, while CalECPA requires the greater protection of a warrant for access to that information, as well as IP addresses.²³¹

3. Notice

Unlike CalECPA’s comprehensive notice scheme, the SCA explicitly requires notice to the target only in one context: when a government entity uses a subpoena or a D order to compel the disclosure of the contents of a communication held in electronic storage more than 180 days by an ECS or an RCS.²³² For all other methods that the SCA regulates—including whenever a warrant is used to obtain contents and whenever non-contents information

227. See *supra* notes 52–56 and accompanying text.

228. CAL. PENAL CODE § 1546(d) (West 2017).

229. See, e.g., Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011); *State v. Earls*, 214 N.J. 564 (2013) (finding seizure of location data requires the protections of a warrant based on the New Jersey Constitution).

230. 18 U.S.C. § 2703(c)(2) (2012); CAL. PENAL CODE § 1546(d) (West 2017).

231. 18 U.S.C. § 2703(c)(2) (2012); CAL. PENAL CODE § 1546(d) (West 2017); see also Liebeskind, *supra* note 4 (noting that the SCA permits subpoena access to payment information, call detail records and IP address information, while CalECPA requires a warrant for that same information).

232. 18 U.S.C. § 2703(b)(1)(B) (2012). Note that notice can be delayed under the SCA for similar reasons as under CalECPA. *Id.* § 2705.

is obtained—the statute either explicitly dispenses with notice, or cases have interpreted the statute to dispense with the need for notice.²³³

Notice is essential to keeping law enforcement officers within the parameters set by a legislative scheme. Without it, targets of investigations may never come to understand that their electronic communication information has been acquired, particularly if the service provider is served with a gag order, which often happens under the federal law.²³⁴ With the exception of defendants in criminal trials in which prosecutors disclose electronic communications data as part of discovery practice, targets cannot challenge improper government access to their digital data without adequate notice of that access. As the next Subsection details, under the federal statute, there are few reasons to bring such challenges, even for good cases.

4. *Sanctions and Remedies*

The SCA provides few remedies. Most notably, it furnishes no statutory suppression remedy to victims of investigations that violate its terms.²³⁵ Respected commentators have viewed the SCA's lack of a suppression remedy as its most significant failing, largely because without the possibility of having evidence against them excluded, criminal defendants lack an incentive to challenge law enforcement practices.²³⁶ Without such challenges, the law fails to develop,²³⁷ not to mention that government practices in violation of the statute likely go unaddressed.²³⁸ The SCA does permit victims of unlawful acquisition to bring a damages claim against a service provider that discloses their communications data in violation of the Act, so long as the provider did not act in good faith.²³⁹

233. The DOJ contends that notice is not required when a warrant is used, which seems odd given that notice is constitutionally required under the Fourth Amendment. *See* DOJ Manual, *supra* note 215, at 133.

234. *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 324–25 (2012).

235. 18 U.S.C. § 2708 (2012). Unlike CalECPA, it also fails to provide for an Attorney General action or for motions to modify orders granted pursuant to it or to destroy information obtained under it.

236. *See, e.g.*, Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1285 (2004); Orin S. Kerr, *Lifting the 'Fog' of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 824–26 (2003).

237. *Cf.* Orin Kerr, *Fourth Amendment Remedies and Development of the Law: A Comment on Camreta v. Greene and Davis v. United States*, 2010–2011 CATO SUP. CT. REV. 237, 239, 248–61 (discussing how a narrowed constitutional exclusionary rule removes the incentive to bring cases and stunts the development of Fourth Amendment law).

238. Freiwald, *supra* note 48, at 361–79; *see also* 18 U.S.C. § 2707 (2012) (providing for the possibility of administrative discipline).

239. 18 U.S.C. § 2707 (2012) (providing for damages).

By comparison, while CalECPA lacks a private cause of action, its suppression remedy and other remedies are sure to make it a more potent deterrent against law enforcement abuse than the SCA. Since CalECPA's passage, law enforcement agencies and other government entities around the state have been scrambling to ensure that their practices are consistent with the statutory mandates.²⁴⁰ In addition, considerable effort was put into amending CalECPA to achieve compromises between the demands of the statute and the actual practices of law enforcement personnel.²⁴¹ There is no question that CalECPA has teeth.

V. CONSIDERATIONS GOING FORWARD—FOR CALECPA AND SIMILAR LAWS

CalECPA clearly provides expansive privacy protection to a wide array of modern electronic communications. Even before practical issues of implementation are considered, however, CalECPA's own terms present questions about how to delineate the statute's coverage. They also challenge seemingly entrenched notions in federal statutory and constitutional law.

A. OPEN ISSUES

What is an electronic communication? ECPA and CalECPA use the same language for this central concept, but that language, though exceptionally broad, is not clear. CalECPA defines an electronic communication as “the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.”²⁴² ECPA uses the same language and then adds a few exclusions.²⁴³ But when does a file, whether it is a music file, a photo, or a spreadsheet, become an electronic communication? Are all electronic files stored in the cloud “electronic communications” because they have been sent over the Internet—attached to communications? What if they are created and transferred without human involvement? What, if anything, does not count as an electronic communication? And if something is not an electronic communication, then what is it and how is it treated?²⁴⁴

240. This is based on conversations the author has had with various law enforcement officials in California.

241. *See supra* notes 117–118.

242. CAL. PENAL CODE § 1546(c) (West 2017).

243. 18 U.S.C. § 2510(15) (2012) (excluding, for example, wire and oral communications and communications from a tracking device from the definition of “electronic communication”).

244. CalECPA's sponsor stated that the new law was designed to institute “clear probable cause warrant requirements for government access to electronic information, including data

CalECPA recognizes that some information stored on or generated by an electronic device does not count as electronic communication information and explicitly protects that information nonetheless.²⁴⁵ But the borderline of an electronic communication—separating what counts from what does not—is still important because CalECPA’s service provider definition, and therefore its scope, relies on its definition of an electronic communication.

Recall that CalECPA service providers furnish their “subscribers or users the ability to send or receive electronic communications,” and include “any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.”²⁴⁶ To comply with CalECPA, government entities need to know whether they are seeking electronic communication information and whether they are compelling disclosures from a covered service provider. With such a broad definition, the scope of “service provider” under CalECPA will depend largely what counts as an electronic communication.²⁴⁷ With the definition of an electronic communication unclear, the scope of “service provider” also remains in question, though clearly it is an expansive term.

Over time, court decisions may clarify the definition of electronic communication. They may also elucidate the dividing line between service providers and non-service providers under CalECPA. Until then, it seems that whenever California government entities seek digitally stored information from companies, they must do so using a CalECPA warrant.

Another area of uncertainty concerns the dividing line between subscriber information and electronic communication information. CalECPA’s definition of electronic communication information explicitly includes “an IP address” when it is “information pertaining to any individual or device participating in

from electronic devices, emails, cloud storage, digital documents, text messages, metadata, and location information.” CAL. ASSEMB. COMM. ON PRIVACY & CONSUMER PROT., BILL ANALYSIS, S.B. 1121, 2015–2016 Leg., Reg. Sess., at 6 (2016), www.leginfo.ca.gov/pub/15-16/bill/sen/sb_1101-1150/sb_1121_cfa_20160620_130429_asm_comm.html [<https://perma.cc/7VTJ-XR3B>]. That certainly indicates broad coverage, but it does not help with borderline cases.

245. CAL. PENAL CODE § 1546(d) (West 2017) (electronic information is electronic communication information or electronic device information).

246. *Id.* § 1546(j). As discussed, that definition is much broader than the comparable definitions in federal law. *See supra* notes 97, 211–213.

247. ECPA further limits the scope of its service providers by using defined terms like remote computing service, 18 U.S.C. § 2711(2) (2012), and electronic communications service providers. 18 U.S.C. § 2510(15) (2012).

the communication”²⁴⁸ But there may be times when an IP address acts like “a subscriber or account number or identifier,” such as when it is a fixed IP address that is attached to a person’s device and does not vary with that person’s communications.²⁴⁹ Will such fixed IP addresses be considered to be “subscriber information,” not subject to CalECPA’s warrant requirement?²⁵⁰ Because of the difference between static information and communications information,²⁵¹ the legal status of IP addresses and related information may depend on their function.

CalECPA clearly applies when California government entities conduct their investigations in California, which, for jurisdictional reasons, will be most of the time. But will there be other contexts in which courts will impose CalECPA’s procedures? What about cases involving California-based witnesses? California-based service providers?²⁵² At the same time, if CalECPA affects interstate commerce unduly, it may fall afoul of the Dormant Commerce Clause.²⁵³

Finally, the status of immunity for providers under CalECPA could be clarified. Recall that CalECPA precludes “any cause of action” against a private company or its agents “for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to [CalECPA].”²⁵⁴ CalECPA’s immunity language directly matches the SCA’s, but

248. CAL. PENAL CODE § 1546(d) (West 2017) (defining electronic communication information to also include “any information about an electronic communication or the use of an electronic communication service”).

249. *See, e.g., In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 120 (E.D. Va. 2011) (“Some networks assign one predefined address to each attached device (‘static’ addressing), whereas others assign addresses from a pool of available addresses (‘dynamic’ addressing”).

250. CAL. PENAL CODE § 1546(l) (West 2017). Recall that the SCA explicitly permits “any temporarily assigned network address” to be acquired with a subpoena. 18 U.S.C. § 2703(c)(2)(E) (2012).

251. *See Bellia & Freiwald, supra note 109.*

252. *See Kearney v. Salomon Smith Barney Inc.*, 39 Cal. 4th 95 (2006) (applying California wiretapping law in a case arising out a Georgia firm’s communications with California clients). I am indebted to Michael Sussmann of Perkins Coie for raising the issue of domestication as it relates to CalECPA.

253. DETERMANN, *supra* note 23, § 1-2:2.3.

254. CAL. PENAL CODE § 1546.4(d) (West 2016). The California Law Review Commission has suggested that “service provider” would be better than “corporation” in the statutory text. It is not a good idea to make immunity hinge on obtaining the statutory designation of service provider, however. Courts will likely view “corporation” as broad enough to encompass anyone targeted by a lawsuit subject to this provision. *See Memorandum from the Cal. L. Revision Comm’n, State and Local Agency Access to Customer Information*

CalECPA lacks the SCA's good faith reliance defense,²⁵⁵ likely because the California law provides no civil cause of action to which that defense seemed necessary.

At least one commentator has suggested that immunity is unavailable to providers who are subject to CalECPA but who do not strictly comply with its terms.²⁵⁶ Because CalECPA places no affirmative obligation on private companies, it is not easy to identify ways that they could run afoul of the law. As opposed to California government entities, who must comply with CalECPA's warrant, notice, and data destruction provisions, nothing in CalECPA explicitly obligates private companies to do anything other than comply with their obligations arising under other law.²⁵⁷ Nonetheless it remains possible that a plaintiff, or group of plaintiffs, could bring a claim under California law if a service provider fails to ensure that the government entity to whom it disclosed information or rendered assistance complied with CalECPA.²⁵⁸ For example, New York has proposed language in a bill modeled on CalECPA that would provide immunity for providing information in accordance with the statutory provisions but then states that "[t]his does not preclude a cause of action for providing records, information, facilities, or other forms of assistance in a manner that is inconsistent with" those provisions.²⁵⁹ The possibility of private lawsuits was not likely on the minds of the many companies that strongly supported CalECPA's passage, though the threat of liability could certainly boost compliance.

from Communication Service Providers (2015 Legislation and Next Steps) at 15 (Nov. 25, 2015), <http://www.clrc.ca.gov/pub/2015/MM15-51.pdf> [<https://perma.cc/2BG8-VCN6>].

255. 18 U.S.C. § 2707(e)(3) (2012) (establishing good faith reliance on court orders, warrants, requests, etc. to be "a complete defense to any civil or criminal action brought under this chapter or any other law").

256. Liebeskind, *supra* note 4 ("Service providers should note that the CalECPA immunity requires strict compliance while the federal ECPA allows for good faith immunity.").

257. Service providers may voluntarily disclose electronic communication information if otherwise lawful. CAL. PENAL CODE § 1546.1(f) (West 2017).

258. See DETERMANN, *supra* note 23, § 6-2:1.2 (discussing unfair business practice claims in California). California's unfair business practice doctrine is more expansive than under federal law, which has itself recently expanded in the privacy context. See generally CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION: PRIVACY LAW AND POLICY (2016) (discussing unfair competition enforcement by the FTC).

259. Assemb. B. No. 1895, 2017 Gen. Assemb., 1st Reg. Sess. § 695.20(4) (N.Y. 2017).

B. IMPACT ON BROADER LEGAL QUESTIONS

CalECPA's uniform, highly protective approach has distinct advantages that cast the deficiencies of other statutory models in a poor light.²⁶⁰ By applying its warrant requirement to metadata, location data, electronic communication content, and electronic device data, CalECPA obviates the need to determine where a piece of information resides, how long it has resided there, and the nature of the provider that stores it. That not only provides the greater privacy protection that users want and need, but it creates a statutory structure that is less amenable to indefensible arbitrariness.

As an example, CalECPA does not distinguish on the basis of historical as opposed to forward-looking, or real-time data, which precludes end runs around stricter laws based on that distinction. As an example of the latter, agents in one case seemed to go out of their way to make sure that the cell phone location data was collected as stored records rather than in real-time, presumably because real-time acquisition was subject to a warrant requirement and they viewed access to historical data as available with an easier-to-obtain D order.²⁶¹ The application requested that the cell phone service provider momentarily store the location data, as it was produced in real-time, and then deliver the newly created "stored records," on an ongoing basis, to the requesting agents, subject to the rules of stored, but not real-time data.²⁶² One judge described the same behavior as based on the "instantaneous storage" theory and denied the government's application under the Stored Communication Act.²⁶³ Because CalECPA treats access to stored (historical) and real-time data the same, it removes the incentive for such maneuvering and properly reflects that historical data can be just as intrusive and revealing as data collected in real time.²⁶⁴

260. Cf. Susan Freiwald & Sylvain Metille, *Reforming Surveillance Law: The Swiss Model*, 28 BERKELEY TECH. L.J. 1261 (2013) (comparing the uniform and broadly protective Swiss statute to more the uneven and less protective ECPA).

261. Freiwald, *supra* note 225, at 894–97. The Fifth Circuit ultimately agreed with the agents that they could obtain the stored records with a D order rather than a warrant. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013).

262. Freiwald, *supra* note 225, at 894–97.

263. *In re Application of the U.S. for an Order Authorizing Prospective and Continuous Release of Cell Site Location Records*, 31 F. Supp. 3d 889, 893 (S.D. Tex. 2014) (denying the government's attempts to have its application approved on the basis of a D order rather than probable cause).

264. *Id.*; see also Freiwald, *supra* note 225, at 896–97 (describing views of judges and academics that historical data can be just as intrusive as prospective data). *But see supra* note 52 (describing the *Carpenter* case, pending at the time of publication).

CalECPA's passage also weakens the force of the arguments in favor of the third-party doctrine.²⁶⁵ The large number of technology companies who vigorously backed CalECPA strongly supports the view that people do not forfeit their privacy interests by using new electronic devices or by storing their digital communications in the cloud. The California law enforcement community's willingness to withhold opposition or even support CalECPA suggests that any disagreement with that view is not too firmly held.²⁶⁶ That support also belies the idea that requiring a warrant for metadata and location data will fundamentally inhibit law enforcement investigations.²⁶⁷

VI. CONCLUSION

CalECPA is on its way to demonstrating that the police and other government entities can do their jobs while respecting the enhanced sensitivity of the data users store with their service providers and on their electronic communications devices. As a much more uniform and highly protective law than those at the federal level and in other states, CalECPA stands out as a model for others interested in reform. Understanding how the new law works—in terms of the strides it has made and the few issues it leaves open—is the first step in getting the word out.

265. CalECPA's passage adds to the chorus of other states who have rejected the third-party doctrine when interpreting their state constitutions. See Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 393–412 (2006) (describing a fifty-state survey of state constitutional application of the third-party doctrine).

266. See, e.g., Barcelona, *supra* note 81.

267. The San Diego Police Officer Association lauded CalECPA (S.B. 178) because it would “strengthen[] community relationships and increase[] transparency without impeding on law enforcement’s ability to serve the needs of their communities.” Letter from Brian R. Marvel, President, San Diego Police Officers Ass’n, to Mark Leno, Senator, Cal. State Senate (Sept. 1, 2015), <https://www.eff.org/document/sdpoa-support-letter-sb-178-calecpa> [<https://perma.cc/5NS3-YZTV>].

DIGITAL EXHAUSTION: NEW LAW FROM THE OLD WORLD

Lothar Determann[†]

ABSTRACT

Ebooks, audio files, video clips, computer programs, and other digital goods have become central to our information society and sharing community. When consumers acquire digital goods, they are usually prompted to accept lengthy and complex contract terms that limit consumers' rights. Scholars and consumer protection associations are worried whether consumers still know what they buy when they click to "buy now"—apparently few do, according to a recent empirical study.¹ While the study was conducted in the new world, consumer protection associations in the old world were already trying cases in German courts, asserting that consumers were misled when they were invited to "buy" digital goods under contract terms that precluded any resale of digital goods. Yet, interestingly, German courts have not been sympathetic to the claims. German courts held that downloads of digital goods other than computer programs do not exhaust distribution rights; consumers cannot own digital goods they download; and, even if they did, they cannot temporarily reproduce them to sell a copy without the storage medium.

In this Article, I provide an introduction to the practical and legal dimension of digital exhaustion; examine the statutory framework in the European Union and the United States in comparison; analyze case law on both sides of Atlantic, including very recent decisions regarding digital goods that have not yet been publicized in the United States; and provide an international perspective on exhaustion across national borders. I then apply the relevant legal principles to a set of common factual scenarios and variations to illustrate the significance of the topic and provide concrete legal results as well as a well-founded policy assessment.

The rules on copyright exhaustion remain very complex and divergent in the United States and the European Union. They differ in both jurisdictions, differ between software and other works, differ depending on transaction terms, differ as to whether reproduction is permissible to sell copies separate from storage media, and differ as to whether exhaustion applies internationally. It is no wonder many consumers do not know what they "buy" when they "buy now."

From a public policy perspective, advocates of digital exhaustion can refer to consumer expectations, public access to works, freedom of commerce, and transaction privacy in favor

DOI: <https://doi.org/10.15779/Z384Q7QQ3C>

© 2018 Lothar Determann.

[†] Professor Dr. Lothar Determann practices technology law at Baker McKenzie LLP in Palo Alto and teaches computer, Internet, and data privacy law at Freie Universität Berlin, University of California, Berkeley School of Law, and Hastings College of the Law, San Francisco. As with all articles, opinions expressed are those of the author only, not his firm's, clients' or others'. The author thanks Rechtsreferendarin Paloma Pietsch, judicial clerk at the OLG Hamburg.

1. Aaron Perzanowski & Chris Jay Hoofnagle, *What We Buy When We Buy Now*, 165 U. PA. L. REV. 315 (2017).

of digital exhaustion—allowing consumers to resell copies of digital works without a need for permission from the copyright owner. Opponents can cite to the interests of copyright owners, freedom of contract principles, and counterproductive disruptions that typically come with legislative changes or courts overruling established statutory interpretations. Worth noting is that German courts have so far largely rejected the concept of digital exhaustion and do not seem to be concerned about consumer confusion, despite the traditionally high standards of consumer protection in Germany. As the topic works through courts in the United States and both sides of the Atlantic consider legislative reform, new world courts and regulators should consider views and findings from old world cases.

TABLE OF CONTENTS

I.	INTRODUCTION.....	180
A.	SCENARIOS AND VARIATIONS.....	182
B.	KEY QUESTIONS.....	182
C.	ROADMAP TO ANSWERS.....	183
II.	COPYRIGHT EXHAUSTION ACCORDING TO U.S. AND EU STATUTORY LAW	183
A.	UNITED STATES COPYRIGHT ACT.....	184
B.	EU DIRECTIVES AND GERMAN COPYRIGHT ACT	184
C.	FUNDAMENTAL SIMILARITIES IN U.S. AND EUROPEAN COPYRIGHT LAW	187
III.	COPYRIGHT EXHAUSTION CASES REGARDING TANGIBLE BOOKS AND MUSIC RECORDS.....	189
A.	BOOKS.....	189
B.	MUSIC ON DISKS	189
C.	SUMMARY.....	190
IV.	SOFTWARE COPYRIGHT CASES IN THE U.S. AND IN THE EU 191	
A.	U.S. CASES	191
B.	EU AND GERMAN CASES	193
C.	SUMMARY.....	195
V.	DOWNLOADED AUDIOBOOKS, MUSIC FILES, AND OTHER DIGITAL GOODS	196
A.	RESALE OF DOWNLOADED MUSIC FILES UNDER <i>REDIGI</i> IN THE UNITED STATES.....	196
B.	RESALE OF DOWNLOADED AUDIOBOOKS IN GERMANY	197
1.	<i>Audiobooks</i>	198
2.	<i>Downloaded Ebooks and Audiobooks in Hamburg</i>	201
3.	<i>CJEU on Exhaustion and Alternations of Storage Media</i>	203
4.	<i>CJEU on Software Versus Other Digital Goods</i>	205
C.	DOWNLOADED VIDEO GAMES IN GERMANY	205
D.	USED EBOOKS IN THE NETHERLANDS	209
E.	CJEU ON ONLINE LENDING OF EBOOKS.....	210
F.	SUMMARY.....	212
VI.	INTERNATIONAL EXHAUSTION.....	213
A.	INTERNATIONAL EXHAUSTION UNDER U.S. COPYRIGHT LAW.....	213
B.	INTERNATIONAL EXHAUSTION IN THE EU	214

VII. U.S. AND EU DIGITAL EXHAUSTION RULES SUMMARIZED AND APPLIED.....	215
A. COPIES OF DIGITAL GOODS ON A USB DRIVE OR CD	215
B. COPIES OF DIGITAL GOODS PREINSTALLED ON COMPUTERS, SMARTPHONES, OR CARS	215
C. DOWNLOADED COPIES OF DIGITAL GOODS	216
VIII. ASSESSMENT AND OUTLOOK	216
A. CONSUMER WELFARE AND CONTRACT TERMS.....	217
B. TANGIBLE VERSUS INTANGIBLE COPIES.....	219
C. SOFTWARE VERSUS OTHER DIGITAL GOODS.....	221
D. TYPE AND VALUE OF STORAGE MEDIUM	222
E. DOMESTIC VERSUS INTERNATIONAL SALES	222
F. OUTLOOK.....	223

I. INTRODUCTION

Ebooks, audio files, video clips, computer programs, and other digital goods have become central to the information society and sharing community. Consumers can buy them on disks, download copies from the web or mobile sites for a limited time or for good, or stream them on demand. In each case, they are prompted to accept lengthy and complex contract terms that limit their rights to resell, lend, or rent digital goods, move them from one device to another (say from a disk to a computer), transfer them with a device they own (be it a computer or car²), bring them with them from another country, or pass them on to their heirs.³

Technologies, marketplaces, and transaction terms are rapidly changing.⁴ Scholars and consumer protection associations are worried whether consumers still know what they buy when they click to “buy now.”⁵ Chris

2. Lothar Determann & Bruce Perens, *Open Cars*, 32 BERKELEY TECH. L.J. 913, 916–17 (2017) (describing the integration of proprietary software into smart and autonomous vehicles).

3. Perzanowski & Hoofnagle, *supra* note 1, at 318 (providing Amazon’s terms for Kindle ebooks as an example).

4. See P.B. Hugenholtz, *Adapting Copyright to the Information Superhighway*, in THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 81 (1996) (discussing the challenges that copyright was facing in the digital networked environment expected at the end of the twentieth century).

5. Perzanowski & Hoofnagle, *supra* note 1.

Hoofnagle and Aaron Perzanowski, who recently conducted an empirical study on this question, found that few consumers fully understood online transactions, and provided U.S. regulators and plaintiffs' lawyers with a road map to bringing lawsuits based on unfair competition laws to force providers of digital goods to better educate consumers about what they buy when they "buy now."⁶ While this study was conducted in the new world, consumer protection associations were already bringing a few such cases in the old world, specifically in Germany,⁷ a country with traditionally high consumer protection standards.⁸ The German associations asserted in a number of complaints that consumers were misled when they were invited to "buy" digital goods under contract terms that prohibited resale. Yet, German judges have not been sympathetic to the claims. German courts held that downloads of digital goods other than computer programs do not exhaust distribution rights; consumers do not become owners of digital goods they download; and even if they did, they cannot temporarily reproduce them to sell a copy separate from the

6. *Id.* at 361–75.

7. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715, 2014 (Ger.); Oberlandesgericht Hamburg [OLG Hamburg] [Higher Regional Court of Hamburg] Apr. 12, 2014, MULTIMEDIA UND RECHT [MMR] 740, 2015 (Ger.); Oberlandesgericht Stuttgart [OLG Stuttgart] [Higher Regional Court of Stuttgart] Mar. 11, 2011, MULTIMEDIA UND RECHT [MMR] 834, 2012 (Ger.).

8. See Andreas Maurer, *Consumer Protection and Social Methods of Continental and Anglo-American Contract Law and the Transnational Outlook*, 14 IND. J. GLOBAL LEGAL STUD. 353, 368 (2007) (stating that consumer protection became dominant in Germany after the enactment of the Standard Contract Terms Act of 1976); see also Eleni Kosta, *Construing the Meaning of "Opt-Out" – An Analysis of the European, U.K. and German Data Protection Legislation*, 1 EUR. DATA PROTECTION L. REV. 16, 28, 30 (2015) (concluding that Germany applied a pro-consumer approach when implementing Article 14 of the EU Data Protection Directive); Oliver Förster & Osama Almughrabi, *Managing the Conflict Between U.S. E-Discovery and the German Data Protection Act*, 36 HASTINGS INT'L & COMP. L. REV. 111 (2013); Klaus Tonner & Kathleen Fangerow, *Directive 2011/83/EU on Consumer Rights: A New Approach to European Consumer Law?*, 1 J. EUR. CONSUMER & MKT. L. 67, 76 (2012) (providing an example of how the implementation of EU Consumer Protection Directive 2011/83/EU decreased strong, preexisting German existing consumer protection standards); Dagmar Coester-Waltjen, *Consumer Protection and General Business Terms*, 3 J. EUR. CONSUMER & MKT. L. 160 (2014) (discussing EU and German law on unfair contract terms); Press Release, Verbraucherzentrale Bundesverband, WhatsApp Must Provide Terms and Conditions in German (May 17, 2016), http://www.vzbv.de/sites/default/files/en_kom_2016-05-13_pm_whatsapp_ibu.pdf (describing how a German consumer protection association won a lawsuit against the messenger service WhatsApp which required WhatsApp's terms and conditions to be provided in German).

storage medium.⁹ The Court of Justice of the European Union (CJEU) has seemed more sympathetic to digital exhaustion, but has so far issued only two decisions with limited scope, one regarding enterprise software and another one regarding national legislatures' right under EU law to permit online lending of ebooks by public libraries.¹⁰ The divergence of court decisions, the confusion in the marketplace, the complexity of the topic, and the controversies among scholars warrants a closer look at the current state of the law on digital exhaustion in the new and old worlds.

A. SCENARIOS AND VARIATIONS

To keep a concrete focus, this Article will address three common scenarios with variations. First, a consumer buys digital goods on a low-cost storage medium (such as a USB drive or a CD). Second, a consumer buys a brand-new computer or car with digital goods preinstalled. Third, a consumer purchases digital goods online and downloads copies to a CD, USB drive, computer, or car. As a variation to all three scenarios, the consumer does not outright buy the digital items for good, but lends, rents, or streams them for a limited period of time. And, as a further variation, the consumer obtains their copies on one side of the Atlantic and wants to dispose of them on the other side.

B. KEY QUESTIONS

In all scenarios and variations, the consumer would like to resell, lend, rent, or stream the digital goods when she is done with them. Ideally, the consumer would like to be able to transfer an electronic copy. But in some cases, a consumer may also be prepared to transfer her digital goods with a device on which the copies are stored, such as a CD, USB drive, computer, or car. Whether she may do as she wants to can depend on specifics of her contract, but usually also on the answer to two key questions concerning digital exhaustion: (1) Does the consumer own the copies? (2) Is the consumer permitted to create a temporary, separate copy of her digital goods on a new

9. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (721, 725), 2014 (Ger.); Oberlandesgericht Hamburg [OLG Hamburg] [Higher Regional Court of Hamburg] Apr. 12, 2014, MULTIMEDIA UND RECHT [MMR] 740 (741, 743), 2015 (Ger.); Oberlandesgericht Stuttgart [OLG Stuttgart] [Higher Regional Court of Stuttgart] Mar. 11, 2011, MULTIMEDIA UND RECHT [MMR] 834 (835), 2012 (Ger.); Oberlandesgericht Stuttgart [OLG Stuttgart] [Higher Regional Court of Stuttgart] Mar. 11, 2011, MULTIMEDIA UND RECHT [MMR] 834 (835), 2012 (Ger.).

10. Case C-128/11, *UsedSoft GmbH v. Oracle Int'l Corp.*, 2012 E.C.R. I-0000, 2012 O.J. (C 287) 16; Case C-174/15, *Vereniging Openbare Bibliotheken v. Stichting Leenrecht*, 2016 EUR-Lex CELEX LEXIS 62015CJ0174 (Nov. 10, 2016).

storage medium so she can sell them without the medium on which they are currently stored?

C. ROADMAP TO ANSWERS

To answer the key questions regarding the scenarios, variations, and broader topic of digital exhaustion laid out in Part I, this Article will examine the current statutory framework in the European Union and United States in Part II, review old law regarding books and records in Part III, proceed to software cases in Part IV, introduce new law on exhaustion pertaining to online downloads of digital goods other than software in Part V, and revisit principles on territoriality and international exhaustion in Part VI. Then, this Article presents answers to the key questions Part VII and subjects them to a critical assessment from a policy perspective in Part VIII. Part IX briefly concludes.

II. COPYRIGHT EXHAUSTION ACCORDING TO U.S. AND EU STATUTORY LAW

U.S. courts conceived the exhaustion principle first in the patent context in 1873,¹¹ then with respect to copyrights and book sales in 1908.¹² Courts coined, and still use, the term “first sale doctrine” even though not only sales, but also gifts, can exhaust distribution rights.¹³ Congress adopted the doctrine quickly into the U.S. Copyright Act in 1909¹⁴ and amended it a few times to its present form.¹⁵ In Europe, courts and statutes tend to refer to “exhaustion” and apply harmonized principles set forth in EU Directives.¹⁶ A brief summary sets the stage for a review of the diverging cases in the new and old worlds.

11. *See* *Adams v. Burke*, 84 U.S. 453, 456 (1873).

12. *See* *Bobbs-Merrill Co. v. Straus*, 210 U.S. 339, 350–51 (1908).

13. PAUL GOLDSTEIN, *GOLDSTEIN ON COPYRIGHT*, § 7.6.1 n.4 (3d ed. Supp. 2017) (“[A] gift of copies or phonorecords will qualify as a ‘first sale’ to the same extent as an actual sale for consideration.”).

14. *See* Copyright Act of 1909, Pub. L. No. 60-349, § 41, 35 Stat. 1075 (repealed 1976).

15. *See* 17 U.S.C. § 109 (2012).

16. *See* Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, art. 4(2), 2001 O.J. (L 167) 10 [hereinafter *EU Copyright Directive*]; Directive 2009/24/EC of the European Parliament and of the Council of April 23, 2009 on the Legal Protection of Computer Programs, art. 4(2), § 17(2), 2009 O.J. (L 111) 16 [hereinafter *EU Software Directive*]; *see also* URHEBERRECHTSGESETZ [URHG] § 69(3) (1965) (Ger.) [hereinafter *German Copyright Act*].

A. UNITED STATES COPYRIGHT ACT

Under the U.S. Copyright Act, copyright owners have the exclusive right to reproduce the copyrighted work, make derivative works based upon it, distribute copies of the work, and display it publicly.¹⁷ But “the owner of a particular copy or phonorecord lawfully made under this title . . . is entitled . . . to sell or otherwise dispose of the possession of that copy or phonorecord.”¹⁸ The owner of a copy may also freely rent or lend her copy, except with respect to phonograms and software.¹⁹ The owner of a copy may generally not reproduce or adapt her copy, except a software copy where this is necessary “as an essential step in the utilization of the computer program,” subject to a number of limitations.²⁰

B. EU DIRECTIVES AND GERMAN COPYRIGHT ACT

Under EU Directives and German national law, copyright owners have the exclusive right to reproduce, distribute, and communicate the protected work to the public.²¹ The EU Copyright Directive provides that “[t]he distribution right shall not be exhausted within the Community in respect of the original or copies of the work, except where the first sale or other transfer of ownership in the Community of that object is made by the rightholder or with his consent.”²² Similarly, under the EU Software Directive “[t]he first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof.”²³ As under U.S. law, owners of copies have only very limited

17. See 17 U.S.C. § 106 (2012).

18. 17 U.S.C. § 109(a) (2012).

19. See 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT §§ 8.12(C), 8.12(C)(1), 8.12(D)(1)(a) (2005).

20. 17 U.S.C. § 117(a)(1) (2012). See Aaron Perzanowski & Jason Schultz, *Reconciling Intellectual and Personal Property*, 90 NOTRE DAME L. REV. 1211, 1225 (2015) (describing how software works have broader adaptation and reproduction rights under the fair use doctrine and other theories); see also Aaron Perzanowski & Jason Schultz, *Legislating Digital Exhaustion*, 29 BERKELEY TECH. L.J. 1535, 1547 (2014).

21. EU Copyright Directive, *supra* note 16, art. 2, art. 3(1), art. 4(1); see also German Copyright Act, *supra* note 16, §§ 15(1)(2), 16, 17, 18, 19, 19a, 20, 21, 22.

22. EU Copyright Directive, *supra* note 16, art. 4(2); see also German Copyright Act, *supra* note 16, § 17(2) (“Where the original or copies of the work have been brought to the market by sale with the consent of the person entitled to distribute them within the territory of the European Union or another state party to the Agreement on the European Economic Area, their dissemination shall be permissible, except by means of rental.”).

23. EU Software Directive, *supra* note 16, art. 4(2); see also German Copyright Act, *supra* note 16, § 69(c)(3) (“Where a copy of a computer program is brought to the market with the

reproduction and adaptation rights under EU law.²⁴ An owner of copyrights under EU law has exclusive rental rights,²⁵ which are not exhausted upon first sale.²⁶ Also, as a matter of EU law, the copyright owner has exclusive “public” lending rights,²⁷ which, like the rental right, are not exhausted by first sale.²⁸ But, EU law permits derogations under national copyright law with respect to exhaustion of public lending rights.²⁹ The German legislature, for example, enacted an exemption: under German copyright law, a first sale regarding a particular copy³⁰ exhausts public lending rights;³¹ the copyright owner is

rightholder’s consent in the area of the European Union or another state party to the Agreement on the European Economic Area by sale, the right of distribution shall exhaust in respect of this copy, with the exception of the rental right . . .”).

24. *See, e.g., German Copyright Act, supra* note 16, § 53(2) (permitting the reproduction of single copies, “for one’s own scientific use,” “for one’s own personal information concerning current affairs if the work was broadcasted,” and for other personal use with regards to “small parts of a released work or individual articles being released in newspapers or periodicals” or where the work “has been out of print for at least two years”).

25. *See* Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on Rental Right and Lending Right and on Certain Rights Related to Copyright in the Field of Intellectual Property, art. 1(1), 3(1), 2006 O.J. (L 376) 28 [hereinafter *EU Rental Directive*].

26. *See id.* art. 1(2). The German Copyright Act states:

[W]here the original or copies of the work have been brought to the market by sale with the consent of the person entitled to distribute them within the territory of the European Union or another state party to the Agreement on the European Economic Area, their dissemination shall be permissible, except by means of rental.

German Copyright Act, supra note 16, § 17(2).

27. *See EU Rental Directive, supra* note 25, art. 1(1), 3(1). This lending right is “public” in the sense that “lending” means “making available for use . . . when it is made through establishments which are accessible to the public.” *Id.* art. 2(1)(b).

28. *See id.* art. 1(2). This exhaustion rule applies only to the “public” lending right in the sense of the EU Rental Directive. An owner of a book can lend it to a friend in a private setting because this does not affect the copyright owner’s ‘public’ lending right. *See id.*

29. *See id.* art. 1(1) (“In accordance with the provisions of this Chapter, Member States shall provide, subject to Article 6, a right to authorise or prohibit the rental and lending of originals and copies of copyright works, and other subject matter as set out in Article 3(1)”; *id.* art. 6(1) (“Member States may derogate from the exclusive right provided for in Article 1 in respect of public lending, provided that at least authors obtain a remuneration for such lending.”).

30. *See German Copyright Act, supra* note 16, § 17(2) (which only excludes the copyright owner’s rental right from exhaustion by first sale); *see also* THOMAS DREIER, GERNOT SCHULZE & LOUISA SPECHT, URHEBERRECHTSGESETZ: URHEBERRECHTSWAHRNEHMUNGSGESETZ, KUNSTURHEBERGESETZ: KOMMENTAR § 17 ¶ 25, 52 (5th ed. 2015) [hereinafter DREIER ET AL., URHG].

31. *See German Copyright Act, supra* note 16, § 17(2) (excluding only the copyright owner’s rental right from exhaustion by first sale); *see also* DREIER ET AL., URHG § 17 ¶ 25, 52.

entitled to remuneration if copies are lent publicly, for example, by a state-owned library.³² As under U.S. law, exceptions apply under EU law with respect to software copies: owners of software copies may not rent them,³³ but they have the right to reproduce and alter their copy as necessary to operate the program.³⁴

32. See *German Copyright Act*, *supra* note 16, § 27(2). When a private owner of the copy lends it to a friend, however, the original owner can do that without paying the copyright owner a remuneration fee. See *id.* § 17(3). Instead, payment is due only when the transfer “directly or indirectly serves profit-making purposes.” *Id.*

33. See *EU Software Directive*, *supra* note 16, art. 4(1)(c) (“Subject to the provisions of Articles 5 and 6, the exclusive rights of the rightholder within the meaning of Article 2 shall include the right to do or to authorise: . . . (c) any form of distribution to the public, including the rental, of the original computer program or of copies thereof.”); *id.* art. 4(2) (“The first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof.”). Thus, under the EU Software Directive, software owners are free to resell or give away their software copy. They can also lend the software copy to someone else, but they cannot rent it since the exclusive rental right of the copyright owner is not affected by first sale but remains with the copyright owner. See also *German Copyright Act*, *supra* note 16, § 69(c)(3). The Act states:

The rightholder shall have the exclusive right to perform or authorise the following acts: . . . any form of distribution of the original of a computer program or of copies thereof, including rental. Where a copy of a computer program is brought to the market with the rightholder’s consent in the area of the European Union or another state party to the Agreement on the European Economic Area by sale, the right of distribution shall exhaust in respect of this copy, with the exception of the rental right . . .

Id. Thus, consistent with the provisions of the EU Software Directive, the German Copyright Act provides for an exhaustion of the copyright owner’s lending right, but not with regards to his rental right. See also DREIER ET AL., URHG § 69(c) ¶ 19.

34. See *EU Software Directive*, *supra* note 16, art. 5(1). The Directive states:

In the absence of specific contractual provisions, the acts referred to in points (a) and (b) of Article 4(1) shall not require authorisation by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.

Id.; see also *id.* art. 4(1). The Directive states:

Subject to the provisions of Articles 5 and 6, the exclusive rights of the rightholder within the meaning of Article 2 shall include the right to do or to authorise: (a) the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole; in so far as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the rightholder; (b) the translation, adaptation, arrangement and any other alteration of a computer program and the

C. FUNDAMENTAL SIMILARITIES IN U.S. AND EUROPEAN COPYRIGHT LAW

In the United States and in Europe, copyright law distinguishes between ownership of copyrights and ownership of the original or copies of a work. An author must fix the work in tangible or electronic form in order to acquire copyrights in the work.³⁵ Upon fixation, copyright ownership attaches to the work separately from its original embodiment (such as a manuscript or painting). If the author sells her original work or a copy, the author does not automatically convey ownership of her copyrights, only ownership of the copy sold.³⁶ Ownership of copies under copyright law does not have to coincide with ownership of the medium on which a copy is stored: You can own a computer on which a lawfully rented video clip or an unlawfully pirated ebook copy resides, which you do not own.

Both under U.S. and EU copyright law, the owner of an authorized copy of a work is entitled to resell her copy. If the copyright owner authorized the creation and first sale of the copy, her consent to a resale is not required. A threshold question, then, is what types of commercial transactions convey ownership of a copy for purposes of copyright law?³⁷ In a sales transaction,

reproduction of the results thereof, without prejudice to the rights of the person who alters the program.

Id.; see also *German Copyright Act*, *supra* note 16, § 69(d)(1). The German Copyright Act states:

Unless provided otherwise by special contractual provisions, the acts referred to in section 69c, numbers 1 and 2, shall not require authorisation by the rightholder if they are necessary for the use of the computer program in accordance with its intended purpose, including for error correction, by any person authorised to use a copy of the program.

Id.; *id.* § 69(c)(1)–(2). This portion of the Act states:

The rightholder shall have the exclusive right to perform or authorise the following acts: 1. the permanent or temporary reproduction, in whole or in part, of a computer program by any means and in any form. Insofar as loading, displaying, running, transmission or storage of the computer program necessitates such reproduction, these actions shall be subject to authorisation by the rightholder; 2. the translation, adaptation, arrangement and other modifications of a computer program, as well as the reproduction of the results thereof. The rights of those persons who adapt the program shall remain unaffected

Id.

35. See NIMMER & NIMMER, *supra* note 19, § 2.03(B).

36. Perzanowski & Schultz, *supra* note 20, at 1217–18.

37. Lothar Determann & Aaron Xavier Fellmeth, *Don't Judge a Sale by Its License: Software Transfers Under the First Sale Doctrine in the United States and the European Community*, 36 U.S.F. L.

the seller receives a lump sum payment and the buyer receives perpetual possession of the item sold. Sales are presumed to convey ownership and resale rights.³⁸ In a gift transaction, the giver transfers perpetual possession and ownership without consideration; gifts are also presumed to convey ownership.³⁹ In a lease or loan, on the other hand, the transfer of possession is time-limited and ownership does not transfer.⁴⁰

The term “license” has different meanings. It can refer to a type of commercial transaction that confers reproduction rights in consideration for royalty payments.⁴¹ The term “license” can also be used as another word for “permission.” In the latter case, a “license” or “permission” is not a type of commercial transaction, but an item of value that one can sell, loan, or rent, or grant ancillary to a sale, lease, or rental arrangement. The existence of a license in the sense of “permission” does not infer a presumption or evidence of a sale or transfer of ownership.⁴²

Ownership grants exclusion rights universally against anyone, whereas commercial transactions are negotiated between parties.⁴³ If parties to a commercial transaction agree that ownership to an item shall not transfer, then it generally will not, unless their contracting freedom is overridden by mandatory laws against contracts of adhesion, unconscionable contracts, unfair consumer contracts, or unreasonable restraints on alienation.⁴⁴

REV. 1, 8–22 (2001) (comparing sale and ownership jurisprudence for tangible property, traditional copyrighted works, and software).

38. *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1108 (9th Cir. 2010) (“If the copyright owners’ initial transfers . . . were first sales, then the defendant’s resales were protected by the first sale doctrine and thus were not copyright infringement.”); *Wall Data Inc. v. L.A. Cty. Sheriff’s Dep’t*, 447 F.3d 769, 785 n.9 (9th Cir. 2006) (“By licensing copies of their computer programs, instead of selling them, software developers maximize the value of their software, minimize their liability, control distribution channels, and limit multiple users on a network from using software simultaneously.”); *DSC Commc’ns Corp. v. Pulse Commc’ns, Inc.*, 170 F.3d 1354, 1360 (Fed. Cir. 1999) (recognizing that a sale transfers ownership).

39. *UMG Recordings v. Troy Augusto*, 628 F.3d 1175, 1182 (9th Cir. 2011).

40. *United States v. Wise*, 550 F.2d 1180, 1191, 1192 (9th Cir. 1977); *Vernor*, 621 F.3d at 1107; *see also* *Determann & Fellmeth*, *supra* note 37, at 20; *Lease*, BLACK’S LAW DICTIONARY (10th ed. 2014).

41. *See* *Determann & Fellmeth*, *supra* note 37, at 13, 20.

42. *See id.*

43. *Compare Loan*, BLACK’S LAW DICTIONARY (10th ed. 2014) (“[A] grant of something for temporary use.”), *with Own*, BLACK’S LAW DICTIONARY (10th ed. 2014) (“[T]o have legal title to.”).

44. *See* Harold C. Havighurst, *Limitations Upon Freedom of Contract*, 1979 ARIZ. ST. L.J. 167, 172 (1979).

Based on these basic rules of U.S. and EU copyright law, consumers must answer two of the three questions introduced above⁴⁵ to determine if and how they can resell their digital goods: (1) Do I own my copy? (2) May I create a temporary, separate copy of my digital good on a new storage medium so I can sell my it without the medium on which my copy happens to be stored (such as a CD, USB drive, computer, or car)?² To develop answers to these two questions with respect to the scenarios and variations introduced above,⁴⁶ Parts II through V of this Article will review old and new cases from both sides of the Atlantic.

III. COPYRIGHT EXHAUSTION CASES REGARDING TANGIBLE BOOKS AND MUSIC RECORDS

A. BOOKS

Booksellers do not usually require customers to sign complex contracts. In a bookstore, customers lay down their money and take their book. They then own the book and can resell, rent, or lend it.⁴⁷ When a book publisher tried to impose license terms on book sales to control resale pricing, the U.S. Supreme Court stepped in and postulated the first sale doctrine for copyrights in 1908.⁴⁸ Since then, books have been sold and resold without much controversy on either side of the Atlantic.⁴⁹

B. MUSIC ON DISKS

Music stores followed booksellers for most of their history. They sold vinyl records, audiotapes, CDs, DVDs, and Blu-ray disks like books, without elaborate contracts. Equally, consumers have been reselling their copies. Controversies have been rare, with a few exceptions such as *UMG Recordings v. Troy Augusto*.⁵⁰ UMG tried to enjoin the resale of promotional CDs with sound recordings that UMG had sent free of charge to music critics subject to a unilateral notice “Promotional Use Only - Not for Sale.”⁵¹ Augusto was not an

45. See *infra* Section I.B.

46. See *infra* Section I.A.

47. See 17 U.S.C. § 109(a) (2012) (guaranteeing these rights in the United States); Copyright, Designs and Patents Act, 1988, c. II, § 18(3)(a) (guaranteeing these rights in the United Kingdom); *German Copyright Act*, *supra* note 16, § 17(2) (guaranteeing these rights in Germany); *EU Copyright Directive*, *supra* note 16, art. 4(2) (guaranteeing these rights in the EU).

48. *Bobbs-Merrill Co. v. Straus*, 210 U.S. 339, 350–51 (1908).

49. Cross-border sales, however, have recently created controversy. See *Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519 (2013).

50. *UMG Recordings v. Troy Augusto*, 628 F.3d 1175 (9th Cir. 2011).

51. *Id.* at 1177. Some disks contained a more elaborate notice:

intended recipient of those CDs, but acquired the CDs and sold them through online auctions at ebay.com.⁵² The court held that UMG's exclusive copyright was exhausted because the distribution of the promotional CDs effected a sale or gift.⁵³ It found no valid license agreement that could have overcome the presumption of a sale or gift, because UMG could not prove that recipients of the promotional CDs expressly or impliedly agreed to any license terms that could have negated a sale or gift.⁵⁴ "[T]ransfer of possession to the recipients, without meaningful control or even knowledge of the status of the CDs after shipment, accomplished a transfer of title."⁵⁵ Moreover, under the Unordered Merchandise Statute, 39 U.S.C. § 3009 (2012), recipients have the right to dispose of the CDs as they see fit.⁵⁶ Courts in the EU would presumably find for exhaustion also under these circumstances, although similar cases do not seem to have been brought. In the U.S., however, the Court of Appeals for the Ninth Circuit had to distinguish *UMG* from software cases. In software cases, U.S. courts tend to defer to the copyright owners' unilateral license terms, including in *Vernor v. Autodesk*⁵⁷—a case decided by the Ninth Circuit around the same time as *UMG*—and in *Wall Data v. L.A. County Sheriff's Department*,⁵⁸ a case it decided only a few years before.⁵⁹

C. SUMMARY

With respect to books and music disks, consumers can answer most questions pertaining to copyright exhaustion and resale rights easily and clearly, whether they are in the United States or in the European Union. Consumers own their copies and can resell them. They do not need—and must not make—any copies for resale purposes. In practice, consumers rarely have to worry about contractual restrictions on their resale rights, because publishers, booksellers, and music stores do not tend to require consumers to execute

This CD is the property of the record company and is licensed to the intended recipient for personal use only. Acceptance of this CD shall constitute an agreement to comply with the terms of the license. Resale or transfer of possession is not allowed and may be punishable under federal and state laws.

Id. at 1182.

52. *Id.* at 1178.

53. *Id.* at 1183.

54. *Id.* at 1180.

55. *Id.* at 1182.

56. *Id.* at 1180.

57. *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1110 (9th Cir. 2010).

58. *Wall Data Inc. v. L.A. Cty. Sheriff's Dep't*, 447 F.3d 769, 785 n.9 (9th Cir. 2006).

59. *UMG Recordings*, 628 F.3d at 1181, 1183.

contracts when they purchase books or music disks. A variety of restrictions apply regarding lending and renting.

IV. SOFTWARE COPYRIGHT CASES IN THE U.S. AND IN THE EU

Software is different in many respects from books.⁶⁰ Software is valuable not for its creativity or originality but for its functionality, which is normally carved out from copyright protection in the U.S.⁶¹ and the EU.⁶² Yet copyright law has become the primary intellectual property regime for software in the U.S. and Europe.⁶³ Both the U.S. and the EU treat software copies differently from copies of other copyrightable works,⁶⁴ but U.S. and EU courts apply the first sale doctrine very differently from each other with respect to software copies.

A. U.S. CASES

In the United States, Congress covered software by copyright with the Computer Software Copyright Act of 1980.⁶⁵ Source and object code is protected as a “literary work”⁶⁶ and, as such, is subject to the same protections and limitations, including the first sale doctrine.⁶⁷ However, where the traditional medium for literary works, such as paperback novels, can be lent out by libraries, Congress saw the risk of libraries lending out valuable software to customers who could then make their own copies and subsequently return the software to the library without ever having paid for it. Therefore, Congress

60. See Christian H. Nandan, *Software Licensing in the 21st Century: Are Software “Licenses” Really Sales, and How Will the Software Industry Respond?*, 32 AIPLA Q.J. 555, 561–63 (2004) (describing how “[s]oftware is fundamentally different than most copyrighted works” because using software requires constantly making new copies of it).

61. 17 U.S.C. § 102(b) (2012).

62. *EU Software Directive*, *supra* note 16, art. 1.2.

63. See Lothar Determann & David Nimmer, *Software Copyright’s Oracle from the Cloud*, 30 BERKELEY TECH. L.J. 161, 165–72 (2015); see also Peter S. Menell, *Tailoring Legal Protection for Computer Software*, 39 STAN. L. REV. 1329, 1354 (1987). See generally Pamela Samuelson, *Comparing U.S. and EC Copyright Protection for Computer Programs: Are They More Different Than They Seem?*, 13 J.L. & COM. 279 (1994) (providing an overview of software copyright protection in the EU).

64. See Part II regarding rental, lending, reproduction and adaptation rights.

65. Act of Dec. 12, 1980, Pub. L. No. 96-517, § 10, 94 Stat. 3028. See also MARK A. LEMLEY, PETER S. MENELL, ROBERT P. MERGES & PAMELA SAMUELSON, *SOFTWARE AND INTERNET LAW* 38–45, 97–98 (1st ed. 2000) (discussing how courts afforded protection to computer programming).

66. See 17 U.S.C. § 101 (2012).

67. *Apple Comput., Inc. v. Franklin Comput. Corp.*, 714 F.2d 1240, 1249 (3d Cir. 1983).

carved out lending and rental of software copies from exhaustion in the Computer Software Rental Amendments Act of 1990.⁶⁸ Owners of software copies may resell their copies according to today's U.S. Copyright Act, but may not lend or rent them out.⁶⁹ In practice, however, software companies have done their utmost to prevent resales, too. They have applied shrinkwrap, click-through, and other software license terms to all software transactions, characterizing transactions as "licenses" and have largely prevailed in U.S. courts with their position that the first sale doctrine should not apply to the distribution of software copies on CDs, even if the acquirer pays a lump sum and acquires perpetual possession of a software copy.⁷⁰ Courts have found it irrelevant that ownership of the CD carrying the software copy does transfer, given the relatively insignificant value of the carrier medium.⁷¹ U.S. courts have largely deferred to contract terms unilaterally imposed by software companies to determine whether end users become owners of their software copies.⁷² Unauthorized software resellers have prevailed with assertions of the first sale doctrine only in situations where the software companies were unable to prove license contract formation and, thus, the first sale doctrine applied by default.⁷³

In most U.S. cases regarding software and exhaustion, copyright owners tried to prevent the resale of software on disks or other carriers of insignificant

68. See Computer Software Rental Amendments Act of 1990, Pub. L. No. 101-650, §§ 801–02, 104 Stat. 5089; Kenneth R. Corsello, *The Computer Software Rental Agreements Act of 1990: Another Bend in the First Sale Doctrine*, 41 CATH. U. L. REV. 177, 180 (1991) ("The Computer Software Rental Amendments Act of 1990 (Software Act) created an exemption from the first sale doctrine for the rental of computer software. This exemption gives the owners of software copyrights control over the rental of their programs by making it a copyright violation to rent computer software without the permission of the copyright owner.").

69. 17 U.S.C. § 109(b) (2012).

70. See Determann & Nimmer, *supra* note 63, at 172–80. *But see* NIMMER & NIMMER, *supra* note 19, § 8.12(B)(1)(d)(i)(III); *SoftMan Prods. Co. v. Adobe Sys. Inc.*, 171 F. Supp. 2d 1075, 1085, 1087 (C.D. Cal. 2001) (examining "the substance of the transaction at issue" and concluding that it "is a sale and not a license").

71. *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1110 (9th Cir. 2010).

72. *Id.*; see, e.g., *Wall Data Inc. v. L.A. Cty. Sheriff's Dep't*, 447 F.3d 769, 785 n.9 (9th Cir. 2006); *DSC Commc'ns Corp. v. Pulse Commc'ns, Inc.*, 170 F.3d 1354, 1360–62 (Fed. Cir. 1999); *MAI Sys. Corp. v. Peak Comput., Inc.*, 991 F.2d 511, 518 (9th Cir. 1993); *Data Prods., Inc. v. Reppart*, 18 U.S.P.Q.2d 1058, 1601 (D. Kan. 1990); *ISC-Bunker Ramo Corp. v. Altech, Inc.*, 765 F. Supp. 1310, 1314 (N.D. Ill. 1990); *Davidson & Assocs., Inc. v. Internet Gateway*, 334 F. Supp. 2d 1164, 1177 (E.D. Mo. 2004); *Microsoft Corp. v. Harmony Computers & Elecs., Inc.*, 846 F. Supp. 208, 213 (E.D.N.Y. 1994); *Novell, Inc. v. Network Trade Ctr., Inc.*, 25 F. Supp. 2d 1218, 1230 (D. Utah 1997).

73. See *Adobe Sys. v. Christenson*, 809 F.3d 1071, 1080 (9th Cir. 2015); *Softman Prods.*, 171 F. Supp. 2d at 1085.

value, not the resale of computers or cars delivered with preinstalled software. In *DSC v. Pulse*, DSC tried to prevent its competitor Pulse from selling devices on which telecommunications companies could upload and run DSC software.⁷⁴ DSC sold its systems to telecommunications companies under agreements that transferred title only to hardware and provided that software copies were only licensed.⁷⁵ The U.S. Court of Appeals for the Federal Circuit decided that users of DSC's systems were not allowed under Section 117 of the U.S. Copyright Act to copy DSC's software onto interoperable devices purchased from Pulse, because DSC effectively reserved ownership to all of its software copies.⁷⁶ But, the court found that Pulse was allowed under Section 117 of the U.S. Copyright Act to execute—and thus copy—DSC's software on systems made by DSC, which Pulse had purchased “on the open market,” thereby apparently assuming that the first sale doctrine must have exhausted DSC's rights to software copies preinstalled on DSC hardware.⁷⁷

Copyright owners regularly reserve ownership to software copies preinstalled on computers, smartphones, cars, and other devices in end-user license terms, but in practice, they have not sued consumers based on copyright law to prevent them from reselling software copies on valuable devices.⁷⁸ Consumers are routinely reselling used automobiles, computers and other devices with preinstalled software copies, which are only licensed, not sold by the copyright owner.

B. EU AND GERMAN CASES

European courts have taken very different views in determining whether software transactions qualify as a sale.⁷⁹ German courts have tended to find sales and exhaustion in all situations where copyright owners parted with copies for good and for a lump sum payment, regardless of whether the copyright owner tried to impose unilateral license terms.⁸⁰ The CJEU has generally been skeptical of copyright law, given copyright law's territoriality

74. *DSC Commc'ns*, 170 F.3d at 1357.

75. *Id.* at 1361–62.

76. *Id.* at 1362.

77. *Id.* at 1363.

78. John A. Rothchild, *The Incredible Shrinking First-Sale Rule: Are Software Resale Limits Lawful?*, 57 RUTGERS L. REV. 1, 22–50 (2004).

79. See Determann & Fellmeth, *supra* note 37, at 105; see also Lothar Determann, *Importing Software and Copyright Law*, 30 COMPUTER & INTERNET LAW. 32, 34–35 (2013).

80. See Lothar Determann, *Notice, Assent Rules for Contract Changes After Douglas v. U.S. District Court*, 12 ELECTRONIC COM. & L. REP. (BNA) 32, 37 (2007); James R. Maxeiner, *Standard-Terms Contracting in the Global Electronic Age: European Alternatives*, 28 YALE J. INT'L L. 109, 167 (2003) (describing German software licensing regimes).

and the CJEU's mission to drive forward the European economic unification and cross border trade within the Common Market.⁸¹

In *UsedSoft v. Oracle*,⁸² Oracle Corporation, a software copyright owner, tried to prevent UsedSoft GmbH from reselling copies of Oracle software that UsedSoft acquired from charities, universities, and other licensees. These organizations had acquired (by download or disk) Oracle software under elaborate license agreements, either at significant discounts or with more licenses than necessary due to Oracle's "license block" pricing practice.⁸³ For example, this practice requires that a licensee who has twenty-seven users would need to purchase two twenty-five-user licenses.⁸⁴ UsedSoft acquired the unused portions of the licenses and marketed them to customers who already had possession of Oracle's software copies and merely needed supplemental licenses for additional users.⁸⁵ Customers who did not already have possession of Oracle's software were able to download the software from Oracle's website after purchasing the license from UsedSoft.⁸⁶ The CJEU held that a software copyright owner may not prevent the resale of software copies that are downloaded over the Internet with the copyright owner's consent.⁸⁷ This holding applies even if the initial acquirer is a business or other sophisticated legal entity and expressly agreed with the software copyright owner that the software copies are licensed only to the initial acquirer and shall not be resold.⁸⁸ Thus, any transfer of possession without a time limit for a lump sum fee constitutes a sale within the meaning of the first sale doctrine.⁸⁹ The CJEU also held that anyone who lawfully acquires a software copy (from the rightholder with their consent or from a secondary distributor after exhaustion) on a disk, on a computer, by way of download, or otherwise, may make an additional copy for purposes of selling such additional copy, so long as the original software copy is deleted or rendered unusable.⁹⁰ Moreover, the CJEU noted

81. See Determann, *supra* note 80, at 34–35.

82. Case C-128/11, *UsedSoft GmbH v. Oracle Int'l Corp.*, 2012 E.C.R. I-0000, 2012 O.J. (C 287) 16. For a detailed analysis of *Oracle v. UsedSoft*, see Louisa Specht's recent work in E-COMMERCE: RECHTSHANDBUCH 566 (Peter Bräutigam & Daniel Rücker eds., 2017).

83. *Id.* at 21–27.

84. *Id.* at 22.

85. *Id.*

86. *Id.* at 26.

87. *Id.* at 44–46; see Determann & Nimmer, *supra* note 63, at 182–83.

88. *UsedSoft GmbH*, at 44–46; see Determann & Nimmer, *supra* note 63, at 182–83.

89. See Determann, *supra* note 80, at 35; see Determann & Nimmer, *supra* note 63, at 182.

90. *UsedSoft GmbH*, at 44–46.

that if copyright exhaustion applies, the secondary purchaser may also transfer licenses⁹¹ and contractual terms to the contrary are unenforceable.⁹²

Since the CJEU applied the first sale doctrine so forcefully in *UsedSoft v. Oracle*, copyright owners have shied away from suing resellers of software that was sold online or on disks—let alone trying to prevent consumers from reselling computers, smartphones, cars, or other valuable devices—in suits based on assertions that the consumers do not own the software copies on such devices. The CJEU’s decision in *UsedSoft v. Oracle* even emboldened an unauthorized reseller of used software licenses in Germany to preemptively sue the software company SAP to obtain a declaratory judgment that SAP’s standard software resale restrictions were invalid. The Regional Court of Hamburg confirmed that such resale restrictions were indeed inconsistent with the first sale doctrine as applied by the CJEU in *UsedSoft v. Oracle* upholding the broad scope of the first sale doctrine applied to software transactions.⁹³

C. SUMMARY

With respect to software copies, users will find it more difficult to answer the questions regarding copyright exhaustion and resale rights, because they often have to consider contract terms. But, as a rule of thumb, users can assume that in the United States, they do not own their copies and they cannot resell, rent, or loan them. In the European Union, users tend to own any copies they acquired in a transaction involving a lump sum payment and perpetual possession, whether they buy their copies on disks or by download; they may resell their copies and even make temporary copies for purposes of resale (so long as they delete their original copy after their transfer), but they may not generally stream or rent software copies.⁹⁴

91. *Id.* at 84–85.

92. *Id.* at 84.

93. Landgericht Hamburg [LG Hamburg] [Regional Court of Hamburg] Oct. 25, 2013, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT RECHTSPRECHUNGS-REPORT REGIONAL [GRUR-RR] 221 (223), 2014 (Ger.); see also Maša Savič, *The Legality of Resale of Digital Content After UsedSoft in Subsequent German and CJEU Case Law*, 37 EUR. INTEL. PROP. REV. 414, 417–18 (2015).

94. *EU Software Directive*, *supra* note 16, art. 4(2) (“The first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof.”); see also DREIER ET AL., URHG § 69(c) ¶ 19; *EU Rental Directive*, *supra* note 25, art. 6.

V. DOWNLOADED AUDIOBOOKS, MUSIC FILES, AND OTHER DIGITAL GOODS

Following the review of cases pertaining to books, music disks, and software in Parts III and IV, this Article will now turn to newer cases regarding other types of digital goods such as audiobooks, ebooks, music files, and video games.

A. RE SALE OF DOWNLOADED MUSIC FILES UNDER *REDIGI* IN THE UNITED STATES

In *Capitol Records, LLC v. ReDigi Inc.*,⁹⁵ the U.S. District Court for the Southern District of New York addressed the issue of resale of digital music files.⁹⁶ ReDigi was an online marketplace for used digital music files.⁹⁷ When users signed up for the ReDigi service, ReDigi enabled them to upload music files from the user's computer or smartphone to ReDigi's server, which was presented as the "Cloud Locker."⁹⁸ Before they were uploaded, a software program confirmed that the music files were authorized copies and not pirated counterfeit.⁹⁹ ReDigi configured its system to ensure that the copy on the user's computer or phone was deleted, bit-by-bit, as the new copy was created in the Cloud Locker, bit-by-bit. Based on this configuration, ReDigi tried to argue that functionally, the same copy was transferred since the system did not permit two full copies to ever exist at the same time.¹⁰⁰ Once the file was in the Cloud Locker, the user could sell it to someone else.¹⁰¹ Whenever a user sold a file, ReDigi transferred a copy to the new owner's Cloud Locker account for download and the previous owner could no longer access her copy.¹⁰² The court held that the resale of the music files on the website of ReDigi infringed the exclusive right of reproduction of Capitol Records under 17 U.S.C. §

95. 934 F. Supp. 2d 640 (S.D.N.Y. 2013).

96. *Id.* at 645.

97. As of this writing, ReDigi appears to have stopped its digital music resale business, and now provides a service website for ebooks under the name "Skoobe." *About*, SKOOBE, <http://shopskoobe.com/about/> (last visited Dec. 31, 2017). ReDigi has also filed an appeal that is currently pending. *See* Brief for Plaintiffs-Appellees, *Capitol Records, LLC v. ReDigi Inc.*, No. 16-2321 (2d Cir. May 5, 2017), 2017 WL 1831835.

98. *Capitol Records*, 934 F. Supp. 2d at 645.

99. *Id.*

100. *Id.* at 645, 650.

101. *Id.* at 646.

102. *Id.*

106(1).¹⁰³ It answered the first two threshold questions as follows: (1) When the user first purchased and downloaded the music file to her computer, the user became the owner and entitled to resell the song with her computer;¹⁰⁴ (2) When the user uploaded a copy of her music file to ReDigi's Cloud Locker, the user infringed the copyright owner's reproduction right, even if ReDigi ensured with its technology that the user's original copy was simultaneously deleted; the new copy in the Cloud Locker was not authorized by the copyright owner, and it did not matter that it functionally took the place of the old copy.¹⁰⁵

Thus, the court did not deny the application of the exhaustion doctrine to digital downloads, it only objected to the unauthorized reproduction that is necessary to transfer a downloaded copy to another storage medium.¹⁰⁶ Based on the *ReDigi* decision, a consumer is generally free to sell her *computer* with a previously downloaded music file based on the U.S. Copyright Act, but may not transfer the files themselves if doing so involves creating copies of them.¹⁰⁷

B. RESALE OF DOWNLOADED AUDIOBOOKS IN GERMANY

After the CJEU wholeheartedly embraced exhaustion with respect to downloaded software copies in *UsedSoft v. Oracle*,¹⁰⁸ national courts in the European Union could have been expected to embrace digital exhaustion for other downloadable digital goods. But German courts took a different view.¹⁰⁹

103. *Id.* at 651; 17 U.S.C. § 106(1) (2012) (“Subject to sections 107 through 122, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies or phonorecords.”).

104. *Capitol Records*, 934 F. Supp. 2d at 655 (“Here, a ReDigi user owns the phonorecord that was created when she purchased and downloaded a song from iTunes to her hard disk.”).

105. *Id.* at 648 (“[C]ourts have not previously addressed whether the unauthorized transfer of a digital music file over the Internet—where only one file exists before and after the transfer—constitutes reproduction within the meaning of the Copyright Act. The Court holds that it does.”).

106. *Id.* at 650 (“[T]he fact that a file has moved from one material object—the user’s computer—to another—the ReDigi server—means that a reproduction has occurred.”).

107. The court did not address potentially applicable contractual restrictions, because it held that the Copyright Act independently prohibited copying. *Id.* at 648.

108. Case C-128/11, *UsedSoft GmbH v. Oracle Int’l Corp.*, 2012 E.C.R. I-0000, 2012 O.J. (C 287) 16.

109. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (721), 2014 (Ger.); Oberlandesgericht Hamburg [OLG Hamburg] [Higher Regional Court of Hamburg] Apr. 12, 2014, MULTIMEDIA UND RECHT [MMR] 740 (741), 2015 (Ger.); Oberlandesgericht Stuttgart [OLG Stuttgart] [Higher Regional Court of Stuttgart] Mar. 11, 2011, MULTIMEDIA UND RECHT [MMR] 834 (835), 2012 (Ger.).

1. *Audiobooks*

In Germany, the Higher Regional Court of Hamm decided on a claim brought by a consumer protection association that license terms by an audiobook provider were unfair because they prohibited consumers from reselling their audiobooks.¹¹⁰ In the *Hamm Audiobooks* case, users could download copies of audiobooks from the defendant's website for payment of a one-time fee by credit card and acceptance of terms according to which the user acquired only a nontransferable right to use the audiobook exclusively for personal use.¹¹¹ The terms also prohibited any commercial use, reproduction, and communicating copies to the public. The court had to decide whether the sales terms were unfair—whether they were unreasonably disadvantageous for the consumer.¹¹² Under German law, consumer protection associations can bring such claims against companies to enjoin them from using unfair or unenforceable contract terms.¹¹³ Standard terms are unenforceable under German law when they are not compatible with essential principles of statutory default provisions from which they deviate.¹¹⁴ Thus, to decide whether terms were unfair, the court had to analyze whether the respective sales terms were inconsistent with German copyright law, in particular the first sale doctrine under section 17(2) of the German Copyright Act.¹¹⁵ The court ruled in favor of the copyright owner, stating that in cases where audiobooks are downloaded from the Internet, the exhaustion doctrine provided by section 17(2) of the

110. Since German courts do not publish cases with names of the litigating parties, this Article will refer to this case as “*Hamm Audiobooks*” for short in text. See Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (716), 2014 (Ger.).

111. *Id.*

112. *Id.*

113. See UNTERLASSUNGSKLAGENGESETZ [UKlaG] [UNFAIR TERMS AND CONDITIONS ACT] § 3 (Ger.).

114. See BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE] § 307(2)(1.) (Ger.).

115. *German Copyright Act*, *supra* note 16, § 17(2). The Act states:

Where the original or copies of the work have been brought to the market by sale with the consent of the person entitled to distribute them within the territory of the European Union or another state party to the Agreement on the European Economic Area, their dissemination shall be permissible, except by means of rental.

Id.

German Copyright Act is not applicable.¹¹⁶ Therefore, the contractual resale prohibitions were enforceable.¹¹⁷

According to the court, a user cannot resell the copy of a media file that the user downloaded from the Internet because the user does not acquire ownership, and exhaustion does not result merely from the online transmission of a file.¹¹⁸ When a company offers audiobooks embodied on a tangible medium, the company engages in distribution and typically transfers ownership of copies.¹¹⁹ Yet, when the same company offers online downloads of an audiobook, the company engages in communication to the public under section 19a German Copyright Act¹²⁰ and not distribution under section 17(1) German Copyright Act.¹²¹ Communication to the public under section 19a¹²² does not result in exhaustion of the distribution right.¹²³

116. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (719), 2014 (Ger.).

117. *Id.*

118. *Id.*

119. *Id.*

120. *German Copyright Act*, *supra* note 16, § 19a (“The right of making works available to the public shall constitute the right to make the work available to the public, either by wire or wireless means, in such a manner that members of the public may access it from a place and at a time individually chosen by them.”).

121. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (720), 2014 (Ger.); *German Copyright Act*, *supra* note 16, § 17(1) (“The right of distribution is the right to offer the original or copies of the work to the public or to bring it to the market.”).

122. *See German Copyright Act*, *supra* note 16, § 19a.

123. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (721), 2014 (Ger.).

The *Hamm Audiobooks* court also noted that Recitals 28¹²⁴ and 29¹²⁵ of the EU Copyright Directive support the view that exhaustion does not occur in cases of online transfers of intangible files.¹²⁶ The court held that outside of the software context, the exhaustion of the distribution right is tied to a transfer of ownership and possession of copies on physical media.¹²⁷ Therefore, a consumer who downloads a copy via the Internet does not acquire ownership of such copy, because physical media does not change hands.¹²⁸ Thus, the court answers the first of our threshold questions regarding exhaustion and resale rights as follows: When the user downloads a copy of an audiobook via the Internet, the user does not become the owner of that copy.

The court also noted that, even if a consumer could acquire ownership of a copy of a digital good by way of download, the consumer could not make an additional copy to sell separate from the computer or smartphone to which she downloaded the file, because doing so would affect the copyright owner's

124. *EU Copyright Directive*, *supra* note 16, recital 28.

Copyright protection under this Directive includes the exclusive right to control distribution of the work incorporated in a tangible article. The first sale in the Community of the original of a work or copies thereof by the rightholder or with his consent exhausts the right to control resale of that object in the Community. This right should not be exhausted in respect of the original or of copies thereof sold by the rightholder or with his consent outside the Community. Rental and lending rights for authors have been established in Directive 92/100/EEC. The distribution right provided for in this Directive is without prejudice to the provisions relating to the rental and lending rights contained in Chapter I of that Directive.

Id.

125. *Id.* recital 29.

The question of exhaustion does not arise in the case of services and on-line services in particular. This also applies with regard to a material copy of a work or other subject-matter made by a user of such a service with the consent of the rightholder. Therefore, the same applies to rental and lending of the original and copies of works or other subject-matter which are services by nature. Unlike CD-ROM or CD-I, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which should be subject to authorisation where the copyright or related right so provides.

Id.

126. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (723), 2014 (Ger.).

127. *Id.* at 725.

128. *Id.* at 726.

reproduction rights.¹²⁹ Therefore, a resale of downloaded copies is not practical, unless users download copies to low-value media, like a USB drive, which most consumers do not do.¹³⁰ Thus, the court's response to the second threshold question on digital exhaustion is: Even if a consumer owns a copy of a digital good other than software, the consumer may not make a temporary copy for purposes of resale, even if the consumer deletes her original copy.

Intrinsic to *Hamm Audiobooks* was the court's answer to the third threshold question regarding the effect and enforceability of applicable contract terms, which it answered as follows: The applicable contract terms prohibiting a resale of downloaded audiobooks were in line with statutory law, did not unfairly limit essential consumer rights, and were therefore enforceable.¹³¹

2. *Downloaded Ebooks and Audiobooks in Hamburg*

Shortly after *Hamm Audiobooks*, the Higher Regional Court of Hamburg¹³² dismissed the appeal of a consumer protection association in a similar case.¹³³ Here, the association also claimed that standard terms for downloads of ebooks and audiobooks offered online were unfair.¹³⁴ According to the challenged terms, consumers did not acquire ownership to copies of downloaded ebooks or audiobooks.¹³⁵ Consumers only acquired a single non-transferable right to download a copy of an ebook or audiobook for personal consumption, which was revocable until receipt of payment in full.¹³⁶ A resale of audiobooks was explicitly prohibited.¹³⁷

Hamburg Audio and Ebooks follows *Hamm Audiobooks*. The court held that when a consumer purchases ebooks or audiobooks, the consumer acquires a right to download and save a copy, but the consumer does not acquire ownership to intangible copies.¹³⁸ Ownership and exhaustion only apply in the

129. *Id.* at 721.

130. *Id.*

131. *Id.* at 727; see BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE] § 307(2)(2) (Ger.).

132. Oberlandesgericht Hamburg [OLG Hamburg] [Higher Regional Court of Hamburg] Apr. 12, 2014, MULTIMEDIA UND RECHT [MMR] 740 (741), 2015 (Ger.). As noted *supra* note 110, since German courts do not list case law by litigant name, this Article will refer to this case as "*Hamburg Audio and Ebooks*," in text. Note that currently a complaint against denial of leave to appeal is pending at the German Supreme Court under file number I ZR 115/15.

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.*

context of tangible media.¹³⁹ Offering an ebook or audiobook for download constitutes “making available to the public” and not distribution.¹⁴⁰ Thus, the doctrine of copyright exhaustion is exclusively applicable to copyrighted works embodied in a tangible medium.¹⁴¹ Exhaustion does not occur when copies are transmitted online;¹⁴² exhaustion requires a transfer of possession of physical media containing a copy.¹⁴³

As the court analyzed the wording of section 17(2) German Copyright Act, it took into account the EU Copyright Directive because national courts in the European Union must interpret national law in compliance with the higher-ranking law of the European Union.¹⁴⁴ Thus, the court referred to Article 4(2) of the EU Copyright Directive,¹⁴⁵ which applies exhaustion in the case of a first sale or other transfer of ownership of an “object.” The Hamburg court concluded that since section 17(2) German Copyright Act is the national codification of Article 4(2) of the EU Copyright Directive, the German statutory provision also applies only to sales of objects—in other words, tangible media.¹⁴⁶ As in *Hamm Audiobooks*, the court found in *Hamburg Audio and Ebooks* that this view was supported by Recital 29 of the EU Copyright Directive.¹⁴⁷ The court noted that this recital expressly states that the exhaustion doctrine cannot apply to sales of intangibles.¹⁴⁸ The court concluded that “distribution” within the meaning of section 17 German Copyright Act requires a sale of a copy on a tangible medium.¹⁴⁹ Sales of ebooks or audiobooks by download therefore do not constitute a distribution and accordingly do not trigger exhaustion.¹⁵⁰

Thus, the court in *Hamburg Audio and Ebooks* answers the three threshold questions pertaining to digital exhaustion similarly to the court in *Hamm*

139. *Id.*

140. *Id.* at 742.

141. *Id.*

142. *Id.* at 741.

143. *Id.*

144. *See EU Copyright Directive, supra* note 16, art. 4(2) (“The distribution right shall not be exhausted within the Community in respect of the original or copies of the work, except where the first sale or other transfer of ownership in the Community of that object is made by the rightholder or with his consent.”).

145. *See id.*

146. Oberlandesgericht Hamburg [OLG Hamburg] [Higher Regional Court of Hamburg] Apr. 12, 2014, MULTIMEDIA UND RECHT [MMR] 740 (741), 2015 (Ger.).

147. *See EU Copyright Act.*

148. Oberlandesgericht Hamburg [OLG Hamburg] [Higher Regional Court of Hamburg] Apr. 12, 2014, MULTIMEDIA UND RECHT [MMR] 740 (742), 2015 (Ger.).

149. *Id.*

150. *Id.*

Audiobooks: Consumers do not become owners of copies they download from the Internet; consumers must not resell such copies or make additional copies for resale purposes; contractual resale restrictions are valid and enforceable.

3. CJEU on Exhaustion and Alternations of Storage Media

The CJEU has not yet had to decide whether exhaustion applies to downloaded audio or ebooks. But the CJEU has opined on the significance of the type of tangible media with respect to generating copies of copyrighted works in *Art & Allposters v. Stichting Pictoright*,¹⁵¹ a case which the CJEU decided shortly before *Hamburg Audio and Ebooks*. Stichting Pictoright, a collective society in the Netherlands, had granted Allposters the right to reproduce works of renowned painters on posters and to distribute such posters.¹⁵² Allposters made and sold posters, as expressly permitted, but also created and sold canvas versions (at a higher price than posters).¹⁵³ Allposters created the canvas products by transferring copies of paintings from posters to canvas via a chemical process.¹⁵⁴ Allposters did not make any additional copies; Allposters only moved the copies from poster paper to canvas background. Unlike in ReDigi's process,¹⁵⁵ Allposters actually moved the physical layer of paint from poster paper to canvas, so that the copy of painting that arrived on canvas was actually physically the same as had existed on poster paper.¹⁵⁶ Nevertheless, Pictoright complained that Allposters' process constituted unlawful reproduction.¹⁵⁷

In *Art & Allposters*, the CJEU had to answer questions primarily concerning the legality of unauthorized alterations to a copy of a work after such copy was made and sold with the consent of the copyright owner. Yet, as a preliminary matter, the CJEU had to opine on the scope and extent of exhaustion, and stated in this regard that "exhaustion of the distribution right applies to the tangible object into which a protected work or its copy is incorporated if it has been placed onto the market with the copyright holder's consent."¹⁵⁸ The CJEU based this statement on three factors: first, on the wording of Article 4(2) of the EU Copyright Directive, which refers to a first

151. C-419/13, *Art & Allposters Int'l BV v. Stichting Pictoright*, 2015 EUR-Lex CELEX LEXIS 62013CJ0419 (Jan. 22, 2015).

152. *Id.*

153. *Id.*

154. *Id.*

155. *See supra* Section V.A.

156. *Art & Allposters Int'l*, 2015 EUR-Lex CELEX LEXIS 62013CJ0419 ¶ 16.

157. *Id.* ¶ 16.

158. *Id.* ¶ 40.

sale or other transfer of ownership of a particular “object”; second, on the wording of Recital 28 of the EU Copyright Directive, which refers to “a tangible article”;¹⁵⁹ and third, a statement of the Contracting Parties of the WIPO Copyright Treaty concerning Articles 6 and 7 of that Treaty, according to which a “copy” refers exclusively to “fixed copies that can be put into circulation as tangible objects.”¹⁶⁰ Thus, the CJEU deduced that distribution rights become exhausted only with respect to a copy on a particular object of physical media (in this case, posters), and that exhaustion does not legitimize subsequent alterations of the physical media (including a transfer from poster paper to canvas).

Since the CJEU emphasized the connection of exhaustion to physical objects, one could infer from *Art & Allposters v. Pictoright* that exhaustion can only be triggered by a transfer of physical objects containing copies of copyrighted works and not by a download of digital copies via the Internet.¹⁶¹ Apply the holding¹⁶² to this Article’s scenarios and variations involving digital downloads, we could conclude:

[E]xhaustion of the distribution right . . . does not apply in a situation where a reproduction of a protected work, after having been marketed in the European Union with the copyright holder’s consent, has undergone an alteration of its medium, such as the transfer of that reproduction from a paper poster onto a canvas, and is placed on the market again in its new form.¹⁶³

In the case of digital copies, the protected work is instead transferred from one computer to another, from a laptop to a phone, or from a tablet to a car.

159. *Id.* ¶ 34

160. *Id.* ¶ 39.

161. See Savič, *supra* note 93, at 425.

162. *Art & Allposters Int’l*, 2015 EUR-Lex CELEX LEXIS 62013CJ0419 ¶ 50. The opinion states:

Article 4(2) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society must be interpreted as meaning that the rule of exhaustion of the distribution right set out in Article 4(2) of Directive 2001/29 does not apply in a situation where a reproduction of a protected work, after having been marketed in the European Union with the copyright holder’s consent, has undergone an alteration of its medium, such as the transfer of that reproduction from a paper poster onto a canvas, and is placed on the market again in its new form.

Id.

163. *Id.* ¶ 50.

This would support German courts' answers to whether consumers may resell downloaded copies of digital goods: they must not resell such copies if doing so alters their physical medium.

4. CJEU on Software Versus Other Digital Goods

In *Hamm Audiobooks* and *Hamburg Audio and Ebooks* both German courts rejected the plaintiffs' arguments that the CJEU's ruling in *UsedSoft v. Oracle* should apply equally to digital goods other than software.¹⁶⁴ The German courts noted that the CJEU's ruling was based on the EU Software Directive, which does not apply to ebooks or audiobooks; which constitutes *lex specialis* with respect to the Copyright Directive; and which does not establish a similar distinction between distribution of copies on tangible media (which can trigger exhaustion) and communication of copies to the public (which cannot trigger exhaustion).¹⁶⁵ Therefore, the German courts concluded that the reasoning of the CJEU in *UsedSoft v. Oracle* cannot be applied to online downloads of digital goods other than software.

C. DOWNLOADED VIDEO GAMES IN GERMANY

In 2010, the German Bundesgerichtshof (Federal Court of Appeals) had to decide on a claim brought by a consumer protection association against an American video game developer in a case commonly referred to as *Half-Life 2*.¹⁶⁶ In this case, consumers had to buy a DVD with a computer program and create an online account to play a video game.¹⁶⁷ To complete the online account creation, consumers had to accept contract terms that prohibited any resale or other transfer of the user account.¹⁶⁸ The consumer association complained that the contract terms prohibiting a resale of online accounts was unfair because it effectively prevented resales of the DVDs with the software, which was in turn inconsistent with the exhaustion principle under German

164. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (724–25), 2014 (Ger.); Oberlandesgericht Hamburg [OLG Hamburg] [Higher Regional Court of Hamburg] Apr. 12, 2014, MULTIMEDIA UND RECHT [MMR] 740 (744), 2015 (Ger.).

165. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (725), 2014 (Ger.); Oberlandesgericht Hamburg [OLG Hamburg] [Higher Regional Court of Hamburg] Apr. 12, 2014, MULTIMEDIA UND RECHT [MMR] 740 (742), 2015 (Ger.).

166. Bundesgerichtshof [BGH] [Federal Court of Justice] Feb. 11, 2010, NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 2661 (2662), 2010 (Ger.) [hereinafter *Half-Life 2*].

167. *Id.* at 2661.

168. *Id.* at 2662.

copyright law.¹⁶⁹ The German court disagreed and noted that the exhaustion principle does not directly apply to online accounts.¹⁷⁰ The German court found the fact that a third party might not be interested in purchasing the DVD without the corresponding online account (because the third party could not use the DVD without the online account) was insufficient to justify expanding the scope of the exhaustion principle or invalidating contract terms.¹⁷¹ The court noted that the first sale of the software DVD triggered exhaustion and the purchaser was free to resell the DVD.¹⁷² Thus, the second purchaser can install the computer program on her computer and, in cases in which the first purchaser did not create an online account, the second purchaser can even create an account and play the video game online.¹⁷³

Five years after *Half-Life 2* and two years after *UsedSoft v. Oracle*, an appellate court in Berlin dismissed an appeal against a decision of the Regional Court of Berlin that ruled on a case with similar to *Half-Life 2*.¹⁷⁴ In the case before the courts in Berlin, users could purchase the video game either on a DVD or download it from the Internet.¹⁷⁵ In either case, users had to install software which they could download from the website of the defendant, create a user account, and accept terms including resale prohibitions.¹⁷⁶ The lower court held that the clauses were enforceable because they did not violate the exhaustion principle and the appeals court affirmed.¹⁷⁷ Citing *Half-Life 2*,¹⁷⁸ the appeals court in Berlin found that the contractual resale prohibitions regarding online accounts did not affect the exhaustion principle applicable to the software copies sold on physical DVDs.¹⁷⁹ Moreover, the court held that

169. *Id.*

170. *Id.* at 2663.

171. *Id.*

172. *Id.*

173. *Id.*

174. Landgericht Berlin [LG Berlin] [Regional Court of Berlin] Jan. 21, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 504, 2014 (Ger.).

175. *Id.*

176. *Id.* at 504–05.

177. *Id.* at 504, 507; Kammergericht Berlin [KG Berlin] [Higher Regional Court of Berlin] Aug. 27, 2015, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 181, 2015 (citing Kammergericht Berlin [KG Berlin] [Higher Regional Court of Berlin] Aug. 10, 2015, MULTIMEDIA UND RECHT [MMR] 340, 2016 (Ger.) (relying on the reasoning in its prior court order in the case).

178. *Half-Life 2*, *supra* note 166, at 2661.

179. Kammergericht Berlin [KG Berlin] [Higher Regional Court of Berlin] Aug. 10, 2015, MULTIMEDIA UND RECHT [MMR] 340 (340), 2016 (Ger.); *see also* Landgericht Berlin [LG

exhaustion did not even apply with respect to copies of video games that users downloaded, because no tangible medium was involved in such cases.¹⁸⁰ The CJEU's reasoning in *UsedSoft v. Oracle* did not apply, because the downloaded video games were not "sold" for purposes of the German copyright law that implemented Article 4(2) of the EU Software Directive.¹⁸¹ In *UsedSoft v. Oracle* the software ran locally and the user received an unlimited right to use the software in exchange for payment of a lump sum fee, whereas in *Half-Life 2*, the program copies of the video games require a constant exchange with the servers of the defendant.¹⁸² The defendant had to provide continuous services to the users to enable them to play the game.¹⁸³ Thus, the user never acquired a position comparable to the one of an owner of the video game.¹⁸⁴ Moreover, the Berlin Court of Appeals noted that the defendant does not offer the games as single copies of works, but rather as an integrated part of a package of services.¹⁸⁵ A transfer of the video game to someone else would factually qualify as a transfer of a contract that requires the consent of the defendant under German law.¹⁸⁶ Thus, no "sale" of a copy in the sense of *UsedSoft v. Oracle* had occurred.¹⁸⁷ As such, when the user purchases video games on DVDs, exhaustion occurs, and the user is free to resell the DVD. However, when the user downloads the video game, no exhaustion occurs since no tangible good is involved.

Two days after the decision of the Regional Court of Berlin,¹⁸⁸ the CJEU decided *Nintendo v. PC Box*.¹⁸⁹ The case was not expressly about exhaustion in cases of video games, but instead about technical measures used to protect

Berlin] [Regional Court of Berlin] Jan. 21, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 504 (508), 2014 (Ger.).

180. Kammergericht Berlin [KG Berlin] [Higher Regional Court of Berlin] Aug. 10, 2015, MULTIMEDIA UND RECHT [MMR] 340 (340), 2016 (Ger.).

181. *Id.*

182. *Id.*

183. *Id.*; see also Landgericht Berlin [LG Berlin] [Regional Court of Berlin] Jan. 21, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 504 (509), 2014 (Ger.).

184. Kammergericht Berlin [KG Berlin] [Higher Regional Court of Berlin] Aug. 10, 2015, MULTIMEDIA UND RECHT [MMR] 340 (340), 2016 (Ger.).

185. *Id.*

186. *Id.*

187. *Id.*

188. Landgericht Berlin [LG Berlin] [Regional Court of Berlin] Jan. 21, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 504 (508), 2014 (Ger.).

189. Case C-355/12, *Nintendo Co. Ltd. v. PC Box Srl*, 2013 EUR-Lex CELEX LEXIS 581 (Sept. 19, 2013).

video games. The CJEU had to decide whether Article 6(3) of the EU Copyright Directive covers only technical protection measures pertaining to media containing copies of works, or also measures on players for such media.¹⁹⁰ Nintendo installed a recognition system in its game consoles and adopted encrypted codes for the cartridges onto which the video games were registered.¹⁹¹ Games without a code cannot normally be used on the consoles.¹⁹² However, when a user installed PC Box equipment on her console, the user could circumvent the protection system and use illegal copies of video games (i.e., games lacking a “Nintendo” code).¹⁹³ In its reasoning, the CJEU did not apply the provisions of the EU Software Directive, under which protection measures may be less far-reaching than the ones under the EU Copyright Directive.¹⁹⁴ The CJEU held that video games are a complex product comprising not only of computer programs, but also of graphic and sound elements which are parts of the video game’s originality and, thus, are protected together with the entire work under the EU Copyright Directive.¹⁹⁵ Hence, the CJEU applies the more protective EU Copyright Directive—rather than the EU Software Directive—to video games.

Later in 2014, the Regional Court of Berlin applied *Nintendo v. PC Box* in the context of exhaustion, video games, and “Keyselling.”¹⁹⁶ An owner of an internet shop sent product keys for video games to customers via email in return of a lump sum fee.¹⁹⁷ The customers could then download video games from the Internet onto their computers.¹⁹⁸ The shop owner claimed that the product keys were added to physical data carriers of the video game which his partners in the United Kingdom and Poland purchased.¹⁹⁹ They would then send him the product keys via email and subsequently destroy the physical data carrier and the electronic copy of the product key in the form of a scanned image file.²⁰⁰ The internet shop owner asserted that the copyright owner’s

190. *Id.* ¶ 18.

191. *Id.*

192. *Id.* ¶ 10–12.

193. *Id.* ¶ 12–14.

194. *Id.* ¶ 21; see also *EU Copyright Directive*, *supra* note 16, art. 6 (providing for broader technological protection measures than article 5(1) and article 6 of EU Software Directive).

195. *Nintendo*, ¶ 23.

196. Landgericht Berlin [LG Berlin] [Regional Court of Berlin] Mar. 11, 2014, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT RECHTSPRECHUNGS-REPORT REGIONAL [GRUR-RR] 490, 2014 (Ger.).

197. *Id.*

198. *Id.*

199. *Id.*

200. *Id.*

“reproduction right was exhausted” and that he was free to resell the product keys.²⁰¹ The court held that exhaustion is tied to the product being sold, but that the internet shop owner changed the form of the product by only selling the product key and not the physical data carrier that had been purchased.²⁰² Thus, the shop owner violated the copyright owner’s reproduction right.²⁰³ The court also stated that nothing else follows from *UsedSoft v. Oracle* because the video games were not downloaded by the first purchaser and, moreover, because video games do not consist exclusively of computer programs.²⁰⁴ The court stated that because of its film elements, the video game enjoys protection under the EU Copyright Directive, and that this finding is supported by the CJEU’s *Nintendo v. PC Box* decision.²⁰⁵ According to the court, however, Article 4(2) of the EU Copyright Directive only provides for exhaustion in cases of tangible media.²⁰⁶ The court then found that there is no reason why a copyright owner should lose the higher protection granted to them by the EU Copyright Directive only because the copyright owner adds a computer program to the protected film elements of a video game.²⁰⁷ This decision by the Regional Court of Berlin affirms the conclusion that *UsedSoft v. Oracle* is not applicable analogously in cases of downloaded video games, and that German courts would find that a download of a video game does not trigger exhaustion since Article 4(2) of the EU Copyright Directive requires the involvement of a tangible good.

D. USED EBOOKS IN THE NETHERLANDS

For comparison, Dutch national copyright law implements the same EU Directives and treaties as German national copyright law and is, thus, generally similar.²⁰⁸ In the Netherlands, a court of appeals seemed more inclined to apply the first sale doctrine than the German courts in Hamm and Hamburg or the U.S. court in *ReDigi*,²⁰⁹ albeit in a preliminary injunction ruling (“kort geding”).²¹⁰ The case involved the online marketplace “Tom Kabinet” for used

201. *Id.*

202. *Id.*

203. *Id.*

204. *Id.* at 491.

205. *Id.*

206. *Id.*

207. *Id.*

208. See P. Bernt Hugenholtz, *Chronicle of the Netherlands: Dutch Copyright Law, 1990-1995*, 169 REVUE INTERNATIONALE DU DROIT D’AUTEUR [R.I.D.A.] 128 (1996).

209. See *supra* Section V.A.

210. Gerechtshof Amsterdam [Amsterdam Court of Appeal] 20 januari 2015, No. 200.154.572/01 SKG (Nederlandse Uitgeversverbond/Tom Kabinet Internet B.V.) (Neth.),

and DRM-free ebooks, using a “one-copy-one-user” model as well as terms resembling ReDigi’s. Under the contract terms of the Tom Kabinet platform, consumers who wanted to sell ebooks had to declare that they had legally acquired their copies and that they would delete their existing copies after uploading a further copy to the platform. In order to prevent trading with illegal copies, the marketplace added new watermarks to the ebooks after they were purchased.²¹¹ The Amsterdam District Court in first instance ruled in the preliminary injunction that the resale of used ebooks could be permissible.²¹² Then, the Amsterdam Court of Appeals agreed with the lower court that the *UsedSoft v. Oracle* decision leaves the question open as to whether digital exhaustion applies to intangible copyrighted work other than software.²¹³ However, since the decision of the Amsterdam Court of Appeals concerned a preliminary injunction, it did not issue a ruling on this issue.²¹⁴ Instead, it left this substantive issue to the court that would eventually decide the case on the merits.²¹⁵ The court ordered that “Tom Kabinet” had to stop the resale of ebooks until the website provided for technical measures that effectively prevented sellers from uploading illegally downloaded copies.²¹⁶

E. CJEU ON ONLINE LENDING OF EBOOKS

In *Vereniging Openbare Bibliotheken v. Stichting Leenrecht*,²¹⁷ in 2016, the CJEU answered questions from a Dutch court on whether Dutch law allowed a

<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHAMS:2015:66> [<https://perma.cc/7KY5-SYVR>] [hereinafter *Tom Kabinet*].

211. See Saba Sluiter, *The Dutch Courts Apply UsedSoft to the 0052 resale of eBooks*, KLUWER COPYRIGHT BLOG (Jan. 28, 2015), <http://kluwercopyrightblog.com/2015/01/28/the-dutch-courts-apply-usedsoft-to-the-resale-of-ebooks/> [<https://perma.cc/B3QL-A94R>].

212. See Loek Essers, *Dutch Courts Lets Ebook Reseller Stay Online*, TECHWORLD (July 22, 2014, 2:54 AM), https://www.techworld.com.au/article/550527/dutch_courts_lets_ebook_reseller_stay_online/ [<https://perma.cc/PAG7-FDHA>].

213. *Tom Kabinet*, *supra* note 210, ¶ 3.5.2.

214. *Id.* ¶ 3.5.3.

215. *Id.*

216. See Sluiter, *supra* note 211; Simon Apel, *Keine Anwendung der “UsedSoft”—Rechtsprechung des EuGH jenseits von Computerprogrammen—Eine Bestandsaufnahme zur Erschöpfung bei “Gebrauchten” Digitalen Gütern*, 2015 ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT (ZUM) 640, 643 (2015).

217. C-174/15, *Vereniging Openbare Bibliotheken v. Stichting Leenrecht*, 2016 EUR-Lex CELEX LEXIS 62015CJ0174 (Nov. 10, 2016). For a critical assessment of the CJEU’s ruling in *Leenrecht*, see Vicky Breemen, *E-Lending According to the ECJ: Focus on Functions and Similar Characteristics in VOB v. Stichting Leenrecht*, 39 EUR. INTELL. PROP. REV. 249 (2017). See also generally Jochen Marly & Anna-Lena Wirz, *Die Weiterverbreitung Digitaler Güter*, 2017 EUROPÄISCHE ZEITSCHRIFT FÜR WIRTSCHAFTSRECHT (EuZW) 16 (analyzing whether digital exhaustion exists in Germany after *Vereniging Openbare Bibliotheken v. Stichting Leenrecht*).

library to lend ebooks by way of temporary downloads under the EU Rental Directive.²¹⁸ In the Dutch case, a public library copied ebooks to a server and allowed library users to download a copy to a personal computer or smartphone.²¹⁹ The Dutch public library ensured that only one copy of the ebook was available to one library user at any given time. After the lending period expired, the lender could no longer access the downloaded copy.²²⁰

The CJEU found no problems with lending ebook copies by way of download. It held that in such cases, “lending” (within the meaning of Art. 1(1),²²¹ Art. 2(1)(b),²²² and Art. 6(1)²²³ of the EU Rental Directive)²²⁴ covered the lending of a digital copy of a book. Under the “one-copy-one-user” model, lending of an ebook affects the copyright owner and the public similarly to lending a physical book.²²⁵ Moreover, the EU court held that a Member State can make the exception to the copyright owner’s exclusive lending right under Art. 6(1) of the Directive, subject to the condition that the ebook that the library is lending has “been put into circulation by a first sale or other transfer of ownership of that copy in the European Union by the holder of the right of distribution to the public or with his consent, for the purpose of Art. 4(2) of Directive 2001/29/EC”²²⁶

Since this decision concludes that an EU Member State may codify an exception to the exclusive lending right of the copyright owner for libraries, it follows that ebooks may fall under the scope of that exception as well. However, the CJEU did not expressly address the question of whether a copyright owner triggers exhaustion by making an ebook available for

218. See *EU Rental Directive*, *supra* note 25.

219. See *EU Copyright Directive*, *supra* note 16, recital 28.

220. Case C-174/15, *Vereniging Openbare Bibliotheken v. Stichting Leenrecht*, 2016 EUR-Lex CELEX LEXIS 62015CJ0174 ¶ 26 (Nov. 10, 2016).

221. *EU Rental Directive*, *supra* note 25, art. 1(1) (“In accordance with the provisions of this Chapter, Member States shall provide, subject to Article 6, a right to authorise or prohibit the rental and lending of originals and copies of copyright works, and other subject matter as set out in Article 3(1).”).

222. *Id.* art. 2(1)(b) (“For the purposes of this Directive the following definitions shall apply: . . . (b) ‘lending’ means making available for use, for a limited period of time and not for direct or indirect economic or commercial advantage, when it is made through establishments which are accessible to the public”).

223. *Id.* art. 6(1) (“Member States may derogate from the exclusive right provided for in Article 1 in respect of public lending, provided that at least authors obtain a remuneration for such lending. Member States shall be free to determine this remuneration taking account of their cultural promotion objectives.”).

224. *Id.*

225. *Vereniging Openbare Bibliotheken*, ¶ 51, 53, 74.

226. *Id.*

download or whether the library could lend a copy that was purchased on a disk or other tangible medium. Thus, the CJEU did not address the threshold question of whether the consumer of a digital good actually owns a copy. The CJEU also did not expressly answer the second threshold question of whether the owner of a copy of a digital good may lend such copy out separate from the media on which it was acquired. Further, the CJEU did not—and did not have to, in the procedural posture of the referral from the Dutch court—expressly address the question of whether reproduction rights of the copyright owner are infringed in the context of digital lending. The mere fact that the CJEU did not raise this issue at all might indicate that the CJEU was not concerned about reproduction rights affected by digital lending. This would also be consistent with its broad views of exhaustion in the context of software downloads, as expressed in *UsedSoft v. Oracle*.²²⁷

F. SUMMARY

When consumers download digital goods other than software in the United States, they may become owners of their copies according to *ReDigi* and are accordingly entitled to resell their copies with the device onto which they downloaded their copies. But consumers are not allowed to transfer copies on a device other than the one they used to first download the copy, even if they quickly or simultaneously delete their original copy. Any such reproduction would constitute copyright infringement under U.S. law. Consequently, buyers of copies of digital goods can resell their copies only on the medium on which they exist (such as on a car or computer), but not separately.

German courts have found that offering digital goods other than software for download does not constitute “distribution,” but instead is “communication to the public.” Communication of intangible copies to the public does not result in exhaustion. As such, users do not become owners of downloaded digital goods, and they must not resell their copies—even with the device on which they downloaded their copies. German courts have also found that owners of digital copies may not transfer their copies without the media on which they are stored, because that infringes the copyright owner’s reproduction rights.

The CJEU also differentiates between the communication of intangible digital goods (which does not trigger exhaustion) and the distribution of tangible digital goods (which does trigger exhaustion) outside the realm of software. But the CJEU does not seem to be concerned with reproduction of

227. See *infra* Section IV.B.

digital copies for purposes of lending (and by extension perhaps of resale), so long as ultimately only one copy per user remains. Yet, the CJEU has not yet ruled on whether offering digital goods other than software for download constitutes distribution (triggering exhaustion) or only communication to the public (which does not trigger exhaustion).

VI. INTERNATIONAL EXHAUSTION

Before turning to our three scenarios and variations to apply our findings regarding digital exhaustion in the new and old worlds, this Article will briefly review the territorial scope of exhaustion in both.

A. INTERNATIONAL EXHAUSTION UNDER U.S. COPYRIGHT LAW

In 2013, the U.S. Supreme Court held in *Kirtsaeng v. John Wiley & Sons, Inc.*,²²⁸ that the first sale doctrine under U.S. copyright law also applies to copies lawfully made and first sold outside the United States.²²⁹ Thus, Kirtsaeng was permitted to buy copies of English textbooks sold under license from a U.S. publisher at low retail prices in Thailand and resell them in the U.S. at a profit in competition with the U.S. publisher, who generally charges higher prices in the U.S. market. Consistent with decade-old prior case law, the lower court held that the first sale doctrine would not apply since no authorized first sale had occurred in the United States.²³⁰ The Supreme Court reversed, stating that so long as copies of copyrighted books were lawfully made and first sold with the copyright owner's permission somewhere in the world, they could be resold in the territory of the United States.²³¹

In *Kirtsaeng*, the U.S. Supreme Court addressed only the sale of physical books, not software or digital goods. But the Court noted the impact of its decision for unauthorized imports of cars and other devices containing software, which the Court wanted to favor.²³² This raises the question of whether the U.S. Supreme Court would also allow the importation of digital goods first sold in Europe on a disk or device or by download. In light of the territoriality principle governing property law, it would seem appropriate for

228. *Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519 (2013).

229. See generally Eric Goldman, *The Supreme Court's Kirtsaeng Ruling is Good News for Consumers, but the First Sale Doctrine is Still Doomed*—Kirtsaeng v. John Wiley, TECH. & MARKETING L. BLOG (Mar. 26, 2013), http://blog.ericgoldman.org/archives/2013/03/the_supreme_cou.htm.

230. *John Wiley & Sons, Inc. v. Kirtsaeng*, 654 F.3d 210 (2d Cir. 2011), *rev'd and remanded*, 568 U.S. 519 (2013).

231. *Kirtsaeng*, 568 U.S. at 558.

232. *Id.* at 542–43.

U.S. courts to decide the question of whether a copyright owner transferred ownership to a copy of a digital good as a matter of U.S. law and not under property laws of the foreign jurisdictions where a copy may have been first acquired.²³³ This would largely preclude reselling in the United States software copies that were acquired abroad because software licensees are usually not considered owners of their copies under *Vernor v. Autodesk, Inc.*,²³⁴ even if they may qualify as owners in Europe under *UsedSoft v. Oracle*.²³⁵ Also, to the extent that reselling or lending a digital copy from Europe to the United States involves reproduction, this would constitute infringement under U.S. law, regardless of whether it may be permissible in Europe.²³⁶ On the other hand, a U.S. court could treat the buyer of a downloaded copy as its owner and allow the resale of an imported car, computer, or USB drive with downloaded music files, if the applicable contract terms are not incompatible with the notion of a sale.

B. INTERNATIONAL EXHAUSTION IN THE EU

Under EU law, the first sale of a copy within any Member State of the European Economic Area (EEA) causes exhaustion and the buyer is free to resell the copy in any EEA member state.²³⁷ But a sale outside the EEA does not count at all. Article 4(2) of the EU Copyright Directive²³⁸ states that “[t]he distribution right shall not be exhausted within the Community . . . except where the first sale or other transfer of ownership in the Community of that object is made by the rightholder or with his consent.” Similarly, Article 4(2) of the EU Software Directive²³⁹ explains that “first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community”²⁴⁰ Thus, if Kirtsaeng sold textbooks purchased in Thailand to students in Germany without the consent of the copyright owner, a German court would have to rule that Kirtsaeng’s resale in Germany infringes the distribution right of the copyright owner. Transactions outside the EEA never exhaust distribution rights within the EEA. Thus, there is no need to consider whether transactions outside the EEA should be analyzed under property laws at the place of transaction or where a resale occurs.

233. Determann, *supra* note 80.

234. *Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1110 (9th Cir. 2010).

235. *See also* Determann, *supra* note 80.

236. *See supra* Section V.A.

237. DREIER ET AL., URHG § 17 ¶ 35.

238. *See EU Copyright Directive, supra* note 16.

239. *See EU Software Directive, supra* note 16.

240. *See EU Copyright Directive, supra* note 16, recital 28.

VII. U.S. AND EU DIGITAL EXHAUSTION RULES SUMMARIZED AND APPLIED

Based on the review of statutes and cases in Parts II through VI of this Article, this Part can answer the questions posed regarding the scenarios and variations set forth in Part I.

A. COPIES OF DIGITAL GOODS ON A USB DRIVE OR CD

If a consumer buys a copy of a digital good on a USB drive or CD, she may generally resell, rent, or lend the USB drive or CD with the copy. If a consumer acquires the copy by way of lending, renting, or streaming, she does not have such rights.

Copies purchased in the European Union can generally be imported and resold in the United States, but not the other way around. U.S. and German courts do not allow the owner of a copy of a digital good to transfer their copy without the storage media, because this would typically infringe the copyright owner's reproduction right.

Exceptions apply with respect to software copies. Renting and lending is generally not allowed in the United States, and reselling is usually effectively prohibited in end-user license agreements, which U.S. courts tend to honor. Courts in the European Union, on the other hand, tend to disregard contractual resale restrictions or license terms, and allow a resale of software copies that a copyright owner transfers perpetually in consideration for a lump sum payment. In the European Union, owners of software copies may also make and sell copies so long as they do not retain an extra copy.

In addition, in the European Union, national copyright law may—and in the Netherlands, does—allow public libraries to lend copies of ebooks so long as only one user has access to each copy at any given time.

In the European Union and the United States, consumers may generally not communicate, perform, or display a rented copy to the public, such as by way of streaming, unless the copyright owner consents.

B. COPIES OF DIGITAL GOODS PREINSTALLED ON COMPUTERS, SMARTPHONES, OR CARS

If a consumer buys digital goods preinstalled on valuable storage devices—such as computers, smartphones or cars—the same rules developed in the preceding section with respect to USB drives and CDs should apply equally. But in practice, copyright owners have not tried to prevent buyers of expensive hardware with preinstalled digital goods from reselling the hardware. Also, car manufacturers generally do not try to prohibit renting and reselling of automobiles based on copyrightable software installed on cars.

C. DOWNLOADED COPIES OF DIGITAL GOODS

If a consumer acquires copies of digital goods online by downloading them, she does not become an owner or obtain resale rights according to German courts, and she may not make an extra copy for purposes of transferring copies she owns separate from the media, even if she deletes the original copy. The exception is software, which may be resold with storage media or copied for separate resale purposes (so long as the original copy is deleted).

According to U.S. courts, consumers typically do not acquire ownership or resale rights with respect to software copies, whether downloaded or acquired on a disk. According to *ReDigi*, consumers may become the owner of a downloaded music file and become permitted to resell the copy with the device on which it was downloaded. But consumers must not create any extra copies for resale purposes, even if they simultaneously delete their original copy.

VIII. ASSESSMENT AND OUTLOOK

The rules on copyright exhaustion remain very complex and divergent in the United States and the European Union. They differ from one jurisdiction to the next, and also differ within each jurisdiction depending on whether software or other digital goods are concerned, whether a first sale occurred within or outside a jurisdiction, and whether copies are downloaded or distributed on physical media. Additional differences are present in each jurisdiction with respect to the validity of contractual resale restrictions, types of commercial transactions, as well as whether reproduction is permissible in order to sell copies separate from storage media and whether exhaustion applies internationally. It is no wonder that many consumers do not know what they “buy” when they “buy now.”²⁴¹

Much has already been written about general policy considerations for and against digital exhaustion. A brief summary of pros and cons seems sufficient for purposes of this Article. Advocates of digital exhaustion refer to consumer expectations, consumer welfare, public access to works, freedom of commerce, and transaction privacy in favor of digital exhaustion, allowing consumers to resell copies of digital works without a need for permission from

241. See Perzanowski & Hoofnagle, *supra* note 1, at 322 (presenting an empirical study on consumers being misled by the “buy now” language in the digital media marketplace).

the copyright owner.²⁴² Opponents cite interests of copyright owners, freedom of contract principles, and counterproductive disruptions that typically come with legislative changes or courts overruling established statutory interpretations.²⁴³

Wherever one comes out on the balancing of public policy interests for and against digital exhaustion, it is worth noting that German courts have, so far, largely rejected the concept of digital exhaustion, despite the traditionally high standards of consumer protection in Germany. This raises the question of whether consumers really need similar litigation in the United States to protect consumer welfare,²⁴⁴ and whether the various other differentiation criteria applied by courts in the United States and in the European Union are appropriate in light of the aforementioned policy considerations.

A. CONSUMER WELFARE AND CONTRACT TERMS

Consumers are not only interested in the ability to resell digital goods, and, perhaps, not even primarily.²⁴⁵ Consumers are usually more focused on their

242. See, e.g., Aaron Perzanowski & Jason Schultz, *Digital Exhaustion*, 58 UCLA L. REV. 889, 893–901 (2011); see also Perzanowski & Schultz, *supra* note 20, at 1213; Joseph P. Liu, *Owning Digital Copies: Copyright Law and the Incidents of Copy Ownership*, 42 WM. & MARY L. REV. 1245, 1303, 1310–11, 1320–21, 1330–33, 1336 (2001); R. Anthony Reese, *The First Sale Doctrine in the Era of Digital Networks*, 44 B.C. L. REV. 577, 585–94 (2003). See generally LAWRENCE LESSIG, *FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY* (2004).

243. See, e.g., Apel, *supra* note 216, at 645–46; see also Herbert Hovenkamp, *Post-Sale Restraints and Competitive Harm: The First Sale Doctrine in Perspective*, 66 N.Y.U. ANN. SURV. AM. L. 487, 490, 493 (2011); see also Peter Mezei, *Digital First Sale Doctrine Ante Portas: Exhaustion in the Online Environment*, 6 J. INTELL. PROP. INFO. TECH. & E-COM. L. 23, 56 (2015) (analyzing arguments against the introduction of a digital exhaustion principle and asserting that digital exhaustion can function effectively when forward-and-delete software is included in the resale of digital goods, as well as unique ID numbers for digital files).

244. Perzanowski & Hoofnagle, *supra* note 1, at 378.

245. See also Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (726), 2014 (Ger.). In *Hamm Audiobooks*, the judges stated that the expectation of the consumer is defined by where and how the consumer wants to use the product and doubt whether the consumer has the expectation to be able to transfer the digital good later.

[The interested consumer will rather make his decision primarily dependent on where and how he wants to use the product – here: the audiobook –, namely whether on the home stationary music system or the local personal computer or on a mobile playback device. For these purposes the different forms of the work are suitable in different ways. It is, therefore, doubtful, whether the possibility of a later transfer acquires significance for the decision on the form of the work. Those who want to give it away as a present will resort to the embodied product anyway.]

ability to use digital goods on several devices (e.g. on a smartphone, home computer, and MP3 music player), to create backup copies in the cloud; to share books, video streams, and music files with family members; and, to copy music libraries to upgraded hardware devices. Neither the first sale doctrine nor other provisions in copyright laws afford consumers such rights, but many suppliers of digital goods grant such rights contractually. Apple's Terms of Use for digital goods, for example, provide that the user may "burn an audio playlist to CD for listening purposes up to seven times,"²⁴⁶ re-download the music file purchased to other devices,²⁴⁷ or upload it to cloud storage.²⁴⁸ Such forms of use, without the respective terms, would violate the rightholder's reproduction right under German and U.S. copyright law. They would not be covered by the first sale doctrine.²⁴⁹ Even if the principle of digital exhaustion was universally accepted, the user would still violate the copyright owner's exclusive reproduction right by, for example, burning the music files from the user's computer on a CD to listen to the music while driving.

Most consumers would appreciate a resale right *in addition* to such contractual rights. But copyright owners may not wish to offer such

Id. (translated by the author).

246. *Apple Media Services Terms and Conditions*, APPLE, <https://www.apple.com/legal/internet-services/itunes/us/terms.html> [<https://perma.cc/U6WF-JGY7>] (describing limitations on "iTunes Store Content") (last updated September 13, 2016).

247. *See id.* ("You may be able to re-download previously acquired Content . . . to your devices that are signed in with the same Apple ID . . ."); *see also Audible Conditions of Use*, AMAZON (July 19, 2017), www.amazon.com/gp/aw/help/id=201987350 [<https://perma.cc/4BH5-STXN>] ("As a convenience to you we may continue to make your purchased content available for re-download through your Service account, but we do not guarantee that such content will be available for re-download and Audible will not be liable to you if it becomes unavailable for further re-download.").

248. *See, e.g.*, APPLE, *supra* note 246 (" iCloud Music Library is an Apple Music feature that allows you to access your matched or uploaded songs, playlists and music videos acquired from Apple Music, the iTunes Store or a third party . . . on your Apple Music-enabled devices. . . . You can upload up to 100,000 songs. Songs acquired from the iTunes Store or Apple Music do not count against this limit.").

249. The first sale doctrine results in an exhaustion of the distribution right, but not of the reproduction right of the copyright owner. S. Zubin Gautam, *The Murky Waters of First Sale: Price Discrimination and Downstream Control in the Wake of Kirtsaeng v. John Wiley & Sons, Inc.*, 29 BERKELEY TECH. L.J. 717, 752 (2014) ("Thus, any redistribution by an initial purchaser of a downloaded digital work would implicate the rights holder's exclusive reproduction right . . . [T]he first sale doctrine's limitation of the exclusive right to distribute copyrighted works is irrelevant in the world of distribution via download because the reproduction right indirectly grants the copyright holder absolute control over distribution of her work."); Brian W. Carver, *Why License Agreements Do Not Control Copy Ownership: First Sales and Essential Copies*, 25 BERKELEY TECH. L.J. 1887, 1937 n.212 (2010) (noting that a purchaser could lawfully resell a work of art, but could not make copies of the artwork and sell those).

contractual rights voluntarily if they are forced to accept the consequences of mandatory digital exhaustion. Contractual reproduction rights paired with mandatory resale rights could seriously amplify the adverse impact on copyright owners' commercialization opportunities, as consumers hold more copies that they can potentially resell in practice. If courts and legislatures mandate digital exhaustion without regard to contract terms and legitimate commercialization interests, as the CJEU did in *UsedSoft*,²⁵⁰ copyright owners may be forced to cut down on voluntarily granting reproduction rights or flee into service models that clearly avoid sales, as they have in the software space.²⁵¹

Therefore, from a consumer welfare perspective, courts and legislatures should respect contract terms and commercial transaction types, as U.S. courts generally have, and as German courts have with respect to digital goods other than software. Courts should refrain from applying the exhaustion principle as rigidly as the CJEU did in *UsedSoft v. Oracle*.

B. TANGIBLE VERSUS INTANGIBLE COPIES

Whether legislatures and courts should differentiate between tangible and intangible copies seems more questionable from a policy perspective. Copyright owners and consumers find downloading more convenient and cheaper than other distribution forms, but the basic transaction terms are often identical, and consumers use downloaded copies similarly to copies they buy on disks. Copyright statutes do not define or expressly address downloads differently from other copies.

Factually, it seems questionable whether downloaded copies of digital goods are less tangible than copies on storage media. Components of software have corporeal form.²⁵² The corporeal body of software takes "the form of massive strings of 'bits'."²⁵³ When the software is embodied on a CD, each "bit" is represented by the presence or absence of a pit on the surface of the CD.²⁵⁴ When software is embodied in a less permanent form, like the hard disk of a computer, the corporeal body takes the form of a "series of magnetic switches, positioned at either 'I' or 'O'."²⁵⁵ Even in cases of electronic transfers or downloads, the software program is still corporeal as it exists in the form of

250. Case C-128/11, *UsedSoft GmbH v. Oracle Int'l Corp.*, 2012 E.C.R. I-0000, 2012 O.J. (C 287) 16.

251. Determann & Nimmer, *supra* note 63, at 165–72.

252. Sarah Green & Djakhongir Saidov, *Software as Goods*, 2007 J. BUS. L. 161, 165.

253. *Id.* at 165.

254. *Id.*

255. *Id.*

a “series of electrical pulses.”²⁵⁶ A closer look reveals changes of matter before, during, and after the download process on the supplier’s server, on cables and connections that make up the Internet, and on the buyer’s device.

Like computer software, downloaded audiobooks, ebooks, and music files consist of physical matter.²⁵⁷ CDs containing music files are stamped with pits in which the information (the music) is stored.²⁵⁸ These pits differentiate between a “1” and a “0” bit of the digital music sequence that is read by a laser.²⁵⁹ The sound is then played accordingly. These pits are physically stamped onto the CD and are material objects.²⁶⁰ Information stored in a magnetic hard drive and solid-state drive is stored in the form of electrical and magnetic signals, so-called “fields.”²⁶¹ They are the electromagnetic representation of material pits.²⁶² Such electrical charges and magnetic fields can be considered as material objects rather than being fixed in the magnetic hard drive or solid-state drive.²⁶³ A music file takes up space on the drive of a computer and can be moved from one place to another, just like computer software. Electromagnetic waves and electrical lines move the fields from one drive to another.²⁶⁴

The court in *Hamm Audiobooks* claimed that a download consists of a transfer of instructions to the purchaser’s operating system on local physical memory.²⁶⁵ In contrast to transfers of tangible media, the court emphasized that in the context of downloads, no “substance” is being shifted.²⁶⁶ The court followed the prevailing opinion in Germany that files—not embodied on a tangible medium—are intangible copies of works.²⁶⁷ But other courts have

256. *Id.*

257. Or, as the Supreme Court of Louisiana in *South Central Bell Telephone Co. v. Barthelemy* stated, they consist of a “certain arrangement of matter . . .” 643 So. 2d 1240, 1246 (La. 1994).

258. James Huguenin-Love, *Song on Wire: A Technical Analysis of ReDigi and the Pre-Owned Digital Media Marketplace*, 4 N.Y.U. J. INTELL. PROP. & ENT. L. 1, 15 (2015).

259. *Id.*

260. *Id.* at 15.

261. *Id.* at 17.

262. *Id.*

263. *Id.* at 20.

264. *Id.* at 17.

265. Oberlandesgericht Hamm [OLG Hamm] [Higher Regional Court of Hamm] May 15, 2014, ZEITSCHRIFT FÜR URHEBER UND MEDIENRECHT—RECHTSPRECHUNGSDIENST [ZUM-RD] 715 (724), 2014 (Ger.).

266. *Id.*

267. See Bundesgerichtshof [BGH] [Federal Court of Justice], Oct. 13, 2015, NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 1094 (1095), 2016 (Ger.) Landgericht Konstanz [LG Konstanz] [Regional Court of Konstanz] May 10, 1996, NEUE

held that software, at least for purposes of taxability, qualifies as tangible personal property. In the United States, the Supreme Court of Louisiana,²⁶⁸ for example, stated that software itself is not merely knowledge, but a certain arrangement of matter that makes a person's computer perform a desired function, and that "this arrangement of matter, physically recorded on some tangible medium, constitutes a corporeal body."²⁶⁹ The court wrote that software is "knowledge recorded in a physical form which has physical existence, takes up space on the tape, disc, or hard drive, makes physical things happen, and can be perceived by the senses."²⁷⁰

The court in *ReDigi* assumed, without much discussion, that a consumer can acquire ownership of a downloaded music file copy as much as of a copy on disks as a matter of U.S. copyright law. Where German courts differentiate between tangible and intangible copies, they seem to be less driven by sound policy considerations, and more by a need to distinguish cases that do not involve software from *UsedSoft v. Oracle* and its unreasonable consequences.

C. SOFTWARE VERSUS OTHER DIGITAL GOODS

From a policy perspective, it is compelling that courts in the United States and in the European Union distinguish between software and other digital

JURISTISCHE WOCHENSCHRIFT [NJW] 2662, 1996 (Ger.); CHRISTINA STRESEMANN ET AL., MÜNCHENER KOMMENTAR ZUM BÜRGERLICHEN GESETZBUCH: BGB [MUNICH COMMENTARY ON THE CIVIL CODE] § 90 at 25 (7th ed. 2015) ("Electronic data and computer programs are, as such, not things, since they lack the definable physicality which is characteristic of the conceptual concept."); *id.* (noting that when a file is embodied in a DVD or other tangible medium however, it is treated as a tangible good); *see also* Bundesgerichtshof [BGH] [Federal Court of Justice] Nov. 15, 2006, NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 2394, 2007 (Ger.) (regarding computer programs stored on a physical data carrier).

268. *S. Cent. Bell Tel. Co. v. Barthelemy*, 643 So. 2d 1240, 1241 (1994). The Supreme Court of Louisiana mainly followed the dissenting opinion of Judge Byrnes in the lower court who argued that "tangible" should be understood to encompass "all things that make up our physical universe, as opposed to 'incorporeals' which are limited to the non-physical world of legal concepts." *See S. Cent. Bell Tel. Co. v. Barthelemy*, 631 So. 2d 1340, 1348 (La. Ct. App. 1994) (Byrnes, J., dissenting) ("The codal terms 'corporeal' and 'incorporeal' ante date the advent of computer technology.").

269. *S. Cent. Bell*, 643 So. 2d at 1246.

270. *Id.* at 1241, 1246. The court also stated that the nature of the software's physical manifestation as corporeal or tangible is not affected by the possibility to transfer it to another medium such as a disk or a computer hard drive, as long as the software is stored in physical form on some tangible object. *See id.* at 1241, 1248. However, the court did not decide whether it would consider construe software as tangible where a physical recording of the software would be kept by the service provider and would be transferred to the customer through telephonic transmission, since that issue was not raised by the facts of the case. *See id.* at 1248 n.7.

goods with respect to copyright exhaustion. The value of software does not lie in creative originality, but in functionality, which copyright law is not intended to protect.²⁷¹ Less compelling is the direction this distinction has taken in the European Union after *UsedSoft v. Oracle*, which prescribed various unreasonable consequences without regard to statutory provisions of the EU Software Directive.²⁷²

D. TYPE AND VALUE OF STORAGE MEDIUM

In practice, copyright owners do not usually try to restrict a resale of valuable storage media such as cars, computers, or smartphones based on arguments that digital goods on such items are only licensed, not sold, even though many such items come with license terms that do actually prohibit resale. But from a copyright policy perspective, such distinction seems questionable because copyright law protects copyrighted works and copies without regard to the value of media on which they may happen to reside. If copyright owners are entitled to control whether they part with copies per sale or “license only” with respect to software on cars, then they should also be entitled to “license only” software on disks they sell. Rights under copyright law and personal property laws are not always fully aligned because it is possible and appropriate that one lawfully owns a device on which a rented video clip or pirated music file may reside.

E. DOMESTIC VERSUS INTERNATIONAL SALES

Countries decide based on foreign trade policy considerations whether they want to allow imports of copies first made or sold abroad. Copyrights and other property rights are territorial in nature and, therefore, neutral on this point. The European Union pursues a closed policy in this respect (“fortress Europe”²⁷³), and the United States opened up only recently based on the *Kirtsaeng* decision of the U.S. Supreme Court, which overruled Congress and longstanding government policy—policy that had opposed the concept of international exhaustion to enable copyright owners to apply different pricing in different territories.²⁷⁴

271. See *supra* Part IV.

272. Lothar Determann & Bill Batchelor, *Used Software Sales and Copyright Exhaustion*, 17 ELECTRONIC COM. & L. REP. (BNA) 2149 (2012).

273. See Lothar Determann, *Adequacy of Data Protection in the USA: Myths and Facts*, 6 INT’L DATA PRIVACY L. 244, 247–48 (2016) (describing “protectionist data transfer restrictions” as part of a regulatory scheme colloquially called “Fortress Europe”).

274. *Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519, 573–74 (2013).

F. OUTLOOK

In the United States, efforts are under way to revive *ReDigi*, but it seems unlikely that the substantive law on digital exhaustion will change any time soon given that it is closely aligned with the Copyright Act and not very different with respect to software and other digital goods. In the European Union, the law on digital exhaustion is very different with respect to software and other digital goods, and could change any time if the CJEU overrules German courts. Yet, on both sides of the Atlantic, it is questionable how much digital exhaustion even matters to most consumers and companies from a practical perspective. Software copyright owners have moved largely to service-based models that do not involve distribution or exhaustion under copyright law in the European Union or the United States.²⁷⁵ Consumers increasingly enjoy movies and music via streaming services, which clearly fall outside the realm of exhaustion. To date, copyright owners have not tried on a large scale to prevent resales of cars, computers, smartphones, or other tangible products of significant value based on copyrights to digital goods installed on such products, and market forces should be strong enough to prevent such attempts.

275. Determann & Nimmer, *supra* note 63, at 165–72; Lothar Determann, *What Happens in the Cloud: Software as a Service and Copyrights*, 29 BERKELEY TECH. L.J. 1092, 1098 (2015).

PATENT POOL OUTSIDERS

Michael Mattioli[†]

ABSTRACT

Individuals who decline to join cooperative groups—outsiders—raise concerns in many areas of law and policy. From trade policy to climate agreements to class action procedures, the fundamental concern is the same: a single member of the group who drops out could weaken the remaining union. This Article analyzes the outsider problem as it affects patents.

The outsider phenomenon has important bearing on patent and antitrust policy. By centralizing and simplifying complex patent licensing deals, patent pools conserve tremendous transaction costs. This allows for the widespread production and competitive sale of many useful technologies, particularly in the consumer electronics industry. Because these transaction-cost savings appear to outweigh the most common competition-related concerns raised by patent pools, antitrust authorities generally view these private groups favorably.

Others are less sanguine. Most patent pools are incomplete: for the technologies they cover, not all relevant patents are included. The reason for this is understandable. Patent holders sometimes believe they can negotiate for higher royalties by declining to join an existing pool. Antitrust regulators are aware of this behavior but do not worry much about it. A growing number of economists and legal scholars believe, however, that this outsider behavior may impose higher costs on pool licensees, detracting from the central benefit that patent pools offer—transaction cost savings. These commentators urge antitrust regulators to regard patent pools with greater caution and skepticism.

These calls for caution, however, are based mostly on theories about how patent pools should work, rather than on empirical studies. Remarkably, little research has been done to shed light on the actual impact of patent pool outsiders. Through an original ethnographic study, this Article seeks to remedy this gap. A set of the most notable and public episodes of outsider behavior were collected from industry press reports, case reports, and historical archives. Crucial new information was then gathered through interviews with lawyers and executives directly involved with the episodes studied.

The study reveals a characteristic of patent pools that has gone unappreciated until now: they subtly but powerfully influence bargains that take place “poolside”—i.e., deals between patent holders and licensees that take place “in the shadow” of the pool. This spillover effect can beneficially limit the power that theorists have assumed outsiders have. This is an unappreciated benefit of cooperation. The theorists, as it turns out, have not used the wrong approach, but rather, have been missing some important parameters.

DOI: <https://doi.org/10.15779/Z383F4KN4H>

© 2018 Michael Mattioli.

[†] Associate Professor of Law, Indiana University Maurer School of Law (Bloomington). I wish to express my thanks to Robert Merges, Mark Janis, Austen Parrish, Brian Broughman, Yvonne Cripps, Marshall Leaffer, Daniel Cole, Brett Frischmann, Michael Madison, Katherine Strandburg, Gideon Parchomovsky, Rebecca Eisenberg, Jorge Contreras, Jay Kesan, and Liza Vertinsky. This Article also would not have been possible without the generous cooperation and participation of research subjects.

To further aid regulators, this Article builds upon its qualitative findings by introducing a new quantitative technique for estimating the cost that a licensee either incurs or saves due to an outsider. Applying this technique to original financial and industry data gathered from research subjects, this Article shows that, counterintuitively, patent licensees are sometimes better off where cooperation among licensors is partial, rather than complete. The inflection point lies where the royalty rate hike that a unified pool would need to charge to draw in an outsider is equal to the transaction costs that licensees would conserve by dealing with a single pool.

This study's revelations have provocative implications that reach beyond patent law. Contrary to conventional wisdom, slightly fragmented property markets may sometimes be preferable to "grand coalitions." There may exist in any given market for complementary patent rights (or other complementary property rights), an optimal level of diffusion of ownership that resides between total diffusion and total concentration. Some cooperation may not only be better than none, but also better than more.

Drawing upon this study, antitrust regulators who must evaluate patent pools can assemble a clearer and more complete understanding of their overall costs and benefits. This Article is also helpful beyond patent law. The ethnographic methodology followed here reveals dynamics between outsiders and groups that theory alone has not captured. Scholars concerned with outsiders in other areas of law and policy can refine and build upon theory by applying a similar ethnographic approach.

TABLE OF CONTENTS

I.	INTRODUCTION	227
II.	BACKGROUND	234
	A. PATENT POOLS, INNOVATION, AND COMPETITION.....	234
	B. THE OUTSIDER QUESTION.....	237
	1. <i>The Concerned View of Outsiders</i>	239
	2. <i>The Sanguine View of Outsiders</i>	244
III.	AN ETHNOGRAPHIC STUDY OF PATENT POOL OUTSIDERS	247
	A. METHODOLOGY.....	247
	B. THE UNAPPRECIATED INFLUENCE OF POOLS.....	249
	C. OUTSIDE THE MPEG-2 PATENT POOL (CASE STUDY).....	256
	D. OUTSIDE THE DVD PATENT POOLS (CASE STUDY).....	263
IV.	ASSESSING THE IMPACT OF OUTSIDERS	271
	A. A METHOD FOR ESTIMATING OUTSIDER COSTS AND BENEFITS.....	272
	B. ESTIMATING THE IMPACT OF OUTSIDERS ON DVD LICENSEES.....	275
	C. THE VIRTUES OF IMPERFECT COOPERATION.....	283
V.	CONCLUSION	284

I. INTRODUCTION

A sense of unraveling is in the air. Scholars and experts in far-flung corners of law and policy are growing concerned that outsiders—individuals who decline to join economic, legal, and social collaborations—will upend important policy goals. Ask an international trade expert about outsiders, and you may learn why Britain’s 2016 decision to withdraw from the European Union could undermine and weaken the remaining federation;¹ ask an expert on climate governance, and you may learn that the United States’ decisions to

1. See Guido Calabresi & Eric S. Fish, *Federalism and Moral Disagreement*, 101 MINN. L. REV. 1, 17 (2016) (discussing the potential impact of weak versus strong central governments on Britain’s decision to leave); Paul Craig, *Brexit: A Drama in Six Acts*, 41 EUR. L. REV. 447, 460 (2016) (discussing some issues plaguing the EU resulting in a “social legitimacy deficit”); Horst Eidenmüller, *Negotiating and Mediating Brexit*, 44 PEPP. L. REV. 39, 49 (2016) (warning of “detrimental long-term consequences for the Union as a whole” were other Member States to follow the pathway that the U.K. has forged).

abstain from key treaties could cause cooperation among other nations to dissolve;² ask commentators in corporate law, meanwhile, and you may hear concerns that a sole creditor can disrupt a cooperative plan to divide an insolvent company's or nation's debts.³ In the grand cathedral of law, the outsider concern has become a resounding echo: a rogue litigant undermines the efficiencies of a class action by objecting to settlement terms;⁴ a solitary property owner causes a nuisance by refusing to cooperate with a neighborhood plan;⁵ a venture capitalist threatens the future of a young company by opportunistically pulling out of a cooperative round of funding;⁶ a reluctant juror stands in the way of a just ruling by rejecting the conclusions

2. See generally Daniel H. Cole, *The Problem of Shared Irresponsibility in International Climate Law*, in DISTRIBUTION OF RESPONSIBILITIES IN INTERNATIONAL LAW 290 (André Nollkaemper & Dov Jacobs eds., 2013) (examining how outsider nations that refused to join the Kyoto Protocol affected the underlying goals of the federation of countries that did join).

3. Mark J. Roe, *The Voting Prohibition in Bond Workouts*, 97 YALE L.J. 232, 238 (1987) (“Even when a single creditor and the firm overcome these impediments, they cannot readily strike their own deal and ignore the other creditors, because value will flow from the consenting creditor to the holdout creditors.”); G. Mitu Gulati & Kenneth N. Klee, *Sovereign Piracy*, 56 BUS. LAW. 635, 636 (2001) (discussing the “holdout creditor” issue in connection with competing interpretations of a discussion of a “pari passu” clause, “a standard clause found in almost all sovereign bond indentures”); Lee C. Buchheit & G. Mitu Gulati, *Sovereign Bonds and the Collective Will*, 51 EMORY L.J. 1317, 1324 (2002) (“Holdout creditors could use this threat of liquidation to extract preferential settlements at the expense of the debtor and the other creditors.”).

4. See Elizabeth Chamblee Burch, *Litigating Together: Social, Moral, and Legal Obligations*, 91 B.U. L. REV. 87, 100 (2011) (discussing class action outsiders); Brian T. Fitzpatrick, *The End of Objector Blackmail?*, 62 VAND. L. REV. 1623, 1624 (2009) (explaining that “[t]he holdout problem in class action litigation” stems from an objector to a settlement); Georgene Vairo, *Is the Class Action Really Dead? Is That Good or Bad for Class Members?*, 64 EMORY L.J. 477, 519 (2014) (discussing situations in which defendants have the right to walk away from a settlement if a threshold percentage of plaintiffs do not participate). See, e.g., *In re Microsoft Corp. Antitrust Litig.*, 185 F. Supp. 2d 519, 521 (D. Md. 2002) (“[Plaintiffs] would have a right to opt out, and, if there were a certain number of opt-outs . . . Microsoft would have the right to withdraw from the settlement.”).

5. See, e.g., Abraham Bell & Gideon Parchomovsky, *Reconfiguring Property in Three Dimensions*, 75 U. CHI. L. REV. 1015, 1040–42 (2008) (discussing nuisance doctrine with respect to holdouts and outsiders).

6. See, e.g., Joseph L. Lemon, Jr., *Don't Let Me Down (Round): Avoiding Illusory Terms in Venture Capital Financing in the Post-Internet Bubble Era*, 39 TEX. J. BUS. L. 1 (2003); Usha Rodrigues & Mike Stegemoller, *Exit, Voice, and Reputation: The Evolution of SPACS*, 37 DEL. J. CORP. L. 849, 856 (2013) (discussing a study of voting procedures in the context of special acquisition corporations that “created what turned out to be a costly holdout right”).

of her fellow jurors.⁷ It seems that outsiders are everywhere, threatening the good that can come from cooperation.⁸

Today, one of the most important debates over outsiders concerns patents. A growing number of economists and legal scholars believe that patent holders who refuse to join patent pools—cooperative licensing clearinghouses—will undermine and sometimes entirely undo the benefits that pools deliver.⁹ Such outsider behavior has been on the rise in recent years.¹⁰ Commentators who subscribe to this theory urge antitrust regulators, who must evaluate patent pools, to regard pools more skeptically than they currently do.¹¹

This “Patent Outsider Theory,” as we might call it, is more provocative than it sounds. Patent pools are important to the consumer technology industry, and by extension, to the entire U.S. economy.¹² That is because they address a big problem: transaction costs. Technology standards that the developed world relies upon, such as LTE data and MPEG streaming video, cannot be commercialized without the permission of many different patent holders.¹³ Because dozens of patent holders often hold essential pieces of the

7. See, e.g., *Influences on the Jury*, 45 GEO. L.J. ANN. REV. CRIM. PROC. 643, 656 (2016) (“A judge who concludes that the jury cannot overcome a deadlock may . . . declare a mistrial.”). See generally Jeffrey Abramson, *Anger at Angry Jurors*, 82 CHI.-KENT L. REV. 591 (2007) (describing a holdout juror’s role in hung juries); Shari Seidman Diamond et al., *Revisiting the Unanimity Requirement: The Behavior of the Non-Unanimous Civil Jury*, 100 NW. U. L. REV. 201 (2006) (providing empirical data on holdout behavior on juries); Alison Markovitz, *Jury Secrecy During Deliberations*, 110 YALE L.J. 1493 (2001) (discussing the relationship between the holdout juror and jury deliberations).

8. Richard Epstein noted insightfully that holdouts and externalities can disrupt an efficient allocation of resources. See generally Richard A. Epstein, *Holdouts, Externalities, and the Single Owner: One More Salute to Ronald Coase*, 36 J.L. & ECON. 553 (1993).

9. See *infra* Section II.B.1.

10. *Id.* (enumerating recent episodes).

11. See, e.g., Reiko Aoki & Sadao Nagaoka, *Coalition Formation for a Consortium Standard through a Standard Body and a Patent Pool: Theory and Evidence from MPEG2, DVD, and 3G* at 2–3 (Inst. of Innovation Research Hitotsubashi Univ., Working Paper No. 05-01, 2005), <http://hermes-ir.lib.hit-u.ac.jp/rs/bitstream/10086/15986/1/070iirWP05-01.pdf> [<https://perma.cc/547A-HXBJ>].

12. See generally Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CALIF. L. REV. 1293 (1996) [hereinafter Merges, *Contracting into Liability Rules*]. For a body of work examining different aspects of patent pools, see, for example, FLOYD L. VAUGHAN, *THE UNITED STATES PATENT SYSTEM* (1956); Michael Mattioli, *Power and Governance in Patent Pools*, 27 HARV. J.L. & TECH. 421 (2014); Robert P. Merges, *Institutions for Intellectual Property Transactions: The Case of Patent Pools*, in *EXPANDING THE BOUNDARIES OF INTELLECTUAL PROPERTY: INNOVATION POLICY FOR THE KNOWLEDGE SOCIETY* 123, 129–30, 132, 144 (Rochelle Dreyfuss et al. eds., 2000) [hereinafter Merges, *The Case of Patent Pools*].

13. In the consumer electronics industry, many of these technologies are standards, such as formats for digital video, wireless data communications, and the like. As of this writing

puzzle, the transaction costs of negotiating a deal with each individually would be phenomenally high.¹⁴ A patent pool addresses this problem by granting manufacturers and service providers permission to use the necessary patents through a single agreement. Licensees agree, in return, to pay standard royalty rates, which the pools divide among the patent holders—i.e., their members. By minimizing the number of licensing transactions that must take place, patent pools reduce transaction costs that would otherwise persist.¹⁵ The benefits are far-reaching. Anyone who has owned a smartphone, video game console, personal health device, or modern television has benefited directly from the work that patent pools do.¹⁶

How could a sole outsider upset this happy state of affairs? Theorists imagine the following: if an important patent holder refused to join a patent pool and demanded greater royalties than it would otherwise receive as a member of that pool—i.e., supracompetitive prices—licensees would have to pay higher royalties than they otherwise would.¹⁷ Those higher royalties would offset at least some of the transaction cost savings the pool provides to those licensees.¹⁸ This might motivate other companies to pull away from the pool. It is easy enough to spin out hypothetical problems that might follow: faced with prohibitively high licensing costs, some would-be licensees might decide to focus on other (less preferred) products and services. With fewer competing manufacturers to purchase goods from, consumers could encounter higher prices. Meanwhile, the reduced patent licensing activity could weaken the

(March 2018), one of the largest patent pool administrators in the country is MPEG LA, a company that oversees thirteen patent pools for various standards and is overseeing the development of a future pool. Many of these pools have formed in just the past five to ten years. For more information, see the MPEG LA website. *Revolutionizing Intellectual Property Rights Management*, MPEG LA, www.mpegla.com/main/Pages/About.aspx [https://perma.cc/LTB8-K2Q9] (last visited Mar. 11, 2018); see also Justin R. Orr, *Patent Aggregation: Models, Harms, and the Limited Role of Antitrust*, 28 BERKELEY TECH. L.J. 525, 553 n.159 (2013) (describing the role of patent pools in producing MPEG technology).

14. See Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 SCIENCE 698, 698–700 (1998); Michael Mattioli, *Communities of Innovation*, 106 NW. U. L. REV. 103, 110–13 (2012) (presenting historical and current case studies of this issue); Carl Shapiro, *Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard Setting*, in 1 INNOVATION POLICY AND THE ECONOMY 119, 124–26 (Adam B. Jaffe et al. eds., 2001).

15. See Robert P. Merges & Michael Mattioli, *Measuring the Costs and Benefits of Patent Pools*, 78 OHIO ST. L.J. 281, 297, 319 (2017) (providing estimates of the transaction costs pools conserve and associated methods of deriving these methods).

16. As explained in Part II, patent pools have facilitated the use of digital video standards that the devices listed in this sentence use. These standards include, for instance, MPEG-2 video, Bluetooth, and LTE.

17. See *infra* Section II.B.1.

18. *Id.*

incentive that patents represent, thus dampening research investments. It brings to mind the old proverb, “for want of a nail, the shoe was lost; for want of a shoe, the horse was lost,” and so on, until a battle, a war, and an entire kingdom are lost, “all for want of a horseshoe nail.”¹⁹ That’s how the theorists see it, at least.

This Article suggests that the theorists have it wrong. This conclusion is drawn from an original set of case studies that reveal new information about real-world constraints that limit the power of patent pool outsiders. Most significantly, by publicizing their royalty rates, patent pools signal information to licensees about the value of patents in the pool, as well as the related *patents outside of the pool*. In addition, the outsider strategy presents considerable risks to patent holders. These factors have not been identified or reported on in the literature on patent pools. The research draws upon news articles, press releases, and court papers that describe important outsider episodes. This Article also uniquely provides deeper insight through information that was captured in semi-structured interviews with lawyers and executives who were directly involved with important episodes where patent holders preferred to license patents outside of pools. In addition to illustrating the constraints that pool outsiders are under, these case studies reveal some unappreciated aspects of patent pools that may be relevant in other cooperative settings. This evidence does not suggest that the theorists have it wrong because they have approached the outsider problem incorrectly, but rather, that they have been missing some important dynamics.

This conclusion has important implications for antitrust policy. As mentioned earlier, antitrust regulators evaluate patent pools because, for all of their benefits, pools can raise competition concerns. The chief concern, as explained in greater depth in Part II of this Article, is that a pool may suppress competition between two substitutive technologies by placing them both within the pool.²⁰ Aware of this risk, antitrust regulators have long sought to weigh the benefits and the costs that individual patent pools offer.²¹ In a 2017 article, Robert Merges and I argued that on average, the benefits of patent pools appear to far exceed their costs.²² Interestingly, antitrust authorities have

19. A notable example of this ancient proverb appears in Benjamin Franklin’s 1758 book, *The Way to Wealth*. BENJAMIN FRANKLIN, *THE WAY TO WEALTH* (1758).

20. See *infra* Section II.A.

21. See, e.g., U.S. DEP’T OF JUST. & FED. TRADE COMM’N, *ANTITRUST ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS: PROMOTING INNOVATION AND COMPETITION* (2007), <https://www.justice.gov/sites/default/files/atr/legacy/2007/07/11/222655.pdf> [<https://perma.cc/Z6C4-2HTM>] [hereinafter DOJ GUIDELINES].

22. Merges & Mattioli, *supra* note 15 (concluding that on average, patent pools do far more good than harm).

long assumed that outsiders are not detrimental to patent pools.²³ In general, the Department of Justice (DOJ) views patent pools favorably. In public advisory notices, the DOJ has expressed its view that, absent any unrelated concerns, antitrust authorities will view some cooperation among patent holders as better than none.²⁴

To sum up: the concern about outsiders voiced by academic theorists is at odds with the long-held (but unsupported) assumptions of antitrust regulators. This Article offers the first empirical view of this topic, and it suggests that the regulators have it right: outsiders do not appear to significantly reduce the transaction costs that patent pools conserve. This information has short-term and long-term value to regulators: in the short-term, it provides empirical support for a long-held assumption that has recently been called into question; in the longer term, it urges against a change in how regulators regard patent pool outsiders in the future. Since the nineteenth century, regulators' attitudes toward patent pools have vacillated pendulum-like, between periods of distrust and periods of favor.²⁵ Although regulators are currently friendly toward pools, the pendulum seems likely to swing backward in the future. To further aid regulators, this Article introduces a new quantitative technique for estimating the real-world cost that a licensee either incurs or saves due to an outsider.

This leads to a second surprising discovery. Drawing upon pricing and pooling information collected from interview subjects involved in major pools, this Article argues that, under some circumstances, slightly fragmented property markets are preferable to “grand coalitions”—i.e., a pool containing all relevant patent holders. This argument assumes that a unified patent pool would need to entice outsiders to join by offering royalties either equal to or

23. *See, e.g.*, Letter from Thomas O. Barnett, Assistant Att’y Gen., Antitrust Div., U.S. Dep’t of Justice, to William F. Dolan & Geoffrey Oliver, Jones Day 7 (Oct. 21, 2008), <https://www.justice.gov/archive/atr/public/busreview/238429.pdf> [<https://perma.cc/6PWN-EEYP>] [hereinafter RFID Business Review Letter] (“Not all owners of potentially blocking patents are currently members of the Consortium—and these owners may never join it—potentially limiting efficiency gains. Failure to realize all potential efficiencies does not mean, however, that the efficiencies created are noncognizable.”). In their communications licensees, patent pools have acknowledged the possibility of outsiders as well. *See, e.g.*, Lucent Techs., Inc. v. Gateway, Inc., No. CIV. 02-2060-B(CAB), 2007 WL 2900484, at *11 (S.D. Cal. Oct. 1, 2007) (“Moreover, the MPEG LA sublicensee agreement explicitly warns that the MPEG LA pool does not necessarily include all the patents necessary to practice the technology and that sublicensee signs the agreement aware of such risks.”).

24. RFID Business Review Letter, *supra* note 23.

25. *See* Michael Mattioli, *Empirical Studies of Patent Pools*, in 2 RESEARCH HANDBOOK ON THE ECONOMICS OF INTELLECTUAL PROPERTY LAW (Peter S. Menell et al. eds., forthcoming 2018).

greater than the royalties outsiders already collect independently.²⁶ Because patent pools typically compensate their members according to simple royalty-division formulas, this implies that a pool would need to deliver proportionally higher royalties to all members. A pool that unifies in this way would charge licensees higher royalty rates than the sum of the individual rates that licensees must pay to a partially complete pool and to an outsider. Stated more simply, complete unification may often be undesirable because it entails the cost of luring in outsiders. Outsiders may not be powerful, but multiplication is. These results should be helpful in advancing the scholarly debate, and more practically, to antitrust policy.

This Article's lessons extend beyond patent law. Considering the widespread concern over outsiders in so many areas of law and policy, this Article shows that an ethnographic approach based upon interviews and novel documentary evidence can add critical information that theoretical models are missing. The argument is not that an economic analysis of outsiders is inappropriate, but rather, that such an analysis can yield more accurate and complete results when the dynamics of the situation are well understood. Experts in other domains far removed from patent and antitrust law may find the approach taken here helpful.

The Article unfolds in three parts: Part II explains the relationship between patent pools and federal policies that promote competition and innovation. Part II builds on and summarizes prior research showing that the benefits of patent pools tend to outweigh their costs. The discussion then turns to the recent concerns over patent pool outsiders through a review of recent economic and legal scholarship. Part III presents a set of case studies of outsider behavior in action. These episodes do not support the theory that outsiders meaningfully detract from the benefits patent pools offer. Importantly, these case studies lay out new findings that help explain why, as regulators have long guessed, patent pools can still be very helpful even when they do not contain all of the essential patents involved. Part IV presents a new method that antitrust regulators can use to assess the impact of outsiders on patent pools. Applying real-world data gathered in this study, the Article yields broad new insights that are helpful to policymakers.

26. Based on the interviews conducted for this Article, the decision to join a patent pool is almost entirely an economic one. Although pool membership may theoretically carry spillover benefits—i.e., constructive working relationships with other companies, signaling to inventors—such benefits do not appear to factor prominently into the decision to join a pool.

II. BACKGROUND

Patent pools can be helpful or harmful: on one hand, they conserve vast transaction costs; on the other hand, they can dampen competition. Most scholarship on patent pools has focused on these potential costs and benefits. Recently, however, some scholars have voiced a new concern: they argue that the primary benefit patent pools offer—transaction cost savings—may not be as robust as most experts believe. As a patent pool becomes more economically important, the incentive will grow for some patent holders to “go it alone.” They predict that this behavior can impose high royalty licensing fees on licensees, thus offsetting the transaction costs that pools conserve.

Outsider behavior appears to be on the rise in patent pools. As one subject interviewed for the study in Part III of this Article stated, “this is happening more and more, as patent pools have higher difficulties attracting patent owners.”²⁷ Whether outsiders are truly a problem for pools and for licensees remains an open question. If antitrust authorities are convinced that outsiders are a concern, however, they may regard patent pools less favorably than they presently do. This Part lays the groundwork for the empirical study presented in Part III by discussing these concerns in greater detail.

A. PATENT POOLS, INNOVATION, AND COMPETITION

John Donne’s oft-quoted line, “no [one] is an island,” aptly captures the role patents play in technology markets.²⁸ Many of the products and services that fuel the U.S. economy today incorporate *thousands* of related patented inventions. A widely-cited 2012 study estimated that the average smartphone, for example, incorporates approximately 250,000 patented technologies.²⁹ A lion’s share of the patents that make up these vast mosaics are owned by technology companies.³⁰

In this environment, patent licensing is important and potentially problematic. In theory, any patent holder that blocks the use of a patent essential to a product or service could impede commercialization of that technology.³¹ Manufacturers and service providers thus must achieve a

27. Email from Subject #3 to author (July 18, 2017) (on file with author).

28. JOHN DONNE, DEVOTIONS UPON EMERGENT OCCASIONS (1624).

29. See RPX Corp., Securities Registration Statement, Amendment No. 3 (Form S-1), at 59 (Apr. 18, 2011), <https://www.sec.gov/Archives/edgar/data/1509432/000119312511101007/ds1a.htm> [<https://perma.cc/8HSA-D2ST>].

30. In this Article, the term “technology companies” refers to companies that specialize in computer hardware and software, as well as related digital devices and services. Readers should note that many patents are owned by universities and nonpracticing entities (“NPEs”) as well.

31. See *infra* Section II.B.1 (explaining this in greater detail).

daunting goal: they must obtain *many* licenses from *many* patent holders. Even for firms with ample capital and resources, the transaction costs required could be steep—so steep, in fact, that the licensing might often not take place.³² Scholars in law and economics sometimes call this unhappy outcome, “The Tragedy of the Anticommons”—a term Rebecca Eisenberg and Michael Heller coined to describe the underuse of patented inventions due to high ex ante costs of aggregating rights.³³

Patent pools address this licensing muddle by serving as clearinghouses.³⁴ Groups of patent holders typically form pools to grant licensees (usually manufacturers) permission to use their sets of related patent rights through unified licenses. Today, most patent pools are administered by independent companies with specialized legal and business expertise. These companies help establish pools and handle the ongoing work of furnishing manufacturers and service providers with licenses, collecting royalty payments from them, and then dividing those funds among patent holders. Two of the most prominent patent pool administrators in the United States are MPEG LA, LLC, based in Denver, and Via Licensing Corporation, located in San Francisco.³⁵

Patent pools deliver considerable benefits to their licensees, patent holders, and consumers. By offering collections of patents under standard licensing terms, they remove the need for manufacturers and service providers to negotiate a *series* of individual licenses.³⁶ Patent holders, meanwhile, can draw a stream of royalties from a potentially large set of licensees. Since the 1850s, this elegant cooperative model has enabled the growth of entire industries, from sewing machines, to steel, to airplanes and cars, to critical drugs and medical procedures, to wireless data, to digital film, to television distribution.³⁷ Today, patent pools are particularly important in the field of consumer technology standards. Anyone who has ever listened to a compact disc, used a

32. This is commonly referred to as “The Complements Problem.” See, e.g., Shapiro, *supra* note 14, at 122–24 (explaining the complements problem as it applies to patents).

33. Heller & Eisenberg, *supra* note 14, at 699–700.

34. See Merges, *Contracting into Liability Rules*, *supra* note 12, at 1319 (discussing the clearinghouse function of pools).

35. See *Current Programs*, MPEG LA, <http://www.mpegla.com/> [<https://perma.cc/ZN6V-WAC3>] (click on “Current Programs”) (last visited Mar. 11, 2018); *Licensing Programs*, VIA LICENSING, <http://www.via-corp.com/us/en/licensing.html> [<https://perma.cc/NFZ6-F5P6>] (last visited Oct. 31, 2017).

36. See Richard J. Gilbert, *Ties That Bind: Policies to Promote (Good) Patent Pools*, 77 ANTITRUST L.J. 1, 8 (2010).

37. See Mattioli, *supra* note 12, at 431–39, 444, 449 (discussing and analyzing the royalty division rules in historical patent pools relating to these technologies); Vaughan, *supra* note 12, at 39–68 (discussing historical pools covering these technologies).

smart phone, owned a video game console, or watched a DVD has directly benefited from the work of patent pools.³⁸

Even in the realm of patent licensing, however, there is no such thing as a free lunch. Alongside the transaction costs that they conserve, patent pools can generate social costs if they are not carefully designed. One such cost can result from reduced competition. Suppose a patent pool includes two patented technologies that do the same thing but in slightly different ways. In antitrust parlance, such technologies are called “substitutes.”³⁹ By bundling two substitute technologies in a single license, a patent pool could charge consumers more for both patents than the sum of what each patent would command in a competitive licensing market.⁴⁰ Considering this possibility, it is unsurprising that patent pools have long been scrutinized by antitrust regulators.⁴¹

Some commentators argue that patent pools can also dampen innovation. A patent pool that requires its members to offer a royalty-free license back to the pool covering any future patents the licensee acquires could, in theory, suppress the incentive of exclusivity that patents ordinarily represent. Some scholars believe that companies subject to such “grant-back” clauses may choose to reduce their innovation investments.⁴² The result could be a net drop in innovation, higher prices for consumers, or both. Because of these possibilities, antitrust regulators and courts have long attempted to determine whether individual pools do more harm than good.⁴³ This has generally been an imprecise, highly qualitative exercise.

38. As explained in Part III of this Article, these products all rely upon MPEG-2 video.

39. See DOJ GUIDELINES, *supra* note 21, at 74–78.

40. See *id.* at 77 (“[A] pool containing substitutable patents, i.e., patents covering technologies that compete with each other and that licensee producers would choose between, may have the anticompetitive effect of increasing the total royalty rate to licensees.”).

41. See Merges & Mattioli, *supra* note 15, at 328, 335–36 (explaining that such scrutiny has lately been ad hoc and qualitative).

42. See *id.* at 59–62 (discussing the potential social welfare costs of grant-backs); U.S. DEPT OF JUST. & FED. TRADE COMM’N, ANTITRUST GUIDELINES FOR THE LICENSING OF INTELLECTUAL PROPERTY 31 (2017), https://www.ftc.gov/system/files/documents/public_statements/1049793/ip_guidelines_2017.pdf [<https://perma.cc/2ZBC-DGAR>] (“Another possible anticompetitive effect of pooling arrangements may occur if the arrangement deters or discourages participants from engaging in research and development, thus retarding innovation.”).

43. See, e.g., DOJ GUIDELINES, *supra* note 21, at 2 (“The Antitrust Division of the U.S. Department of Justice and the U.S. Federal Trade Commission (the ‘Agencies’) frequently address complex antitrust questions related to conduct involving the exercise of intellectual property rights in enforcement actions, reports, testimony, reviews of proposed business conduct, and *amicus curiae* or ‘friend of the court’ briefs filed in the federal courts of appeals and the Supreme Court.”). For a discussion of the DOJ’s view of patent pools, see *id.* at 8–9.

In a 2017 article, Robert Merges and I sought to aid regulators in this regard by providing the first empirically grounded estimates of the costs and benefits of patent pools.⁴⁴ We first presented original methods of calculating the transaction cost savings that pools provide and the potential social costs they impose. We then applied those methods to financial data we obtained directly from leading patent pool administrators. Ultimately, we concluded that the transaction costs that modern patent pools conserve appear to greatly exceed the potential social costs they might impose. We estimated that a patent pool organized around popular video and audio standards saves the consumer electronics industry conservatively between \$400 million and \$600 million dollars.⁴⁵ On the other side of the equation, potential costs associated with lost competition or innovation appear to be far lower.⁴⁶ Patent pools might not deliver a “free lunch,” but they look like a remarkably good bargain.

B. THE OUTSIDER QUESTION

Recent scholarship has shown that most modern patent pools do not include *all* of the patents that relate to the technologies they support.⁴⁷ Anne Layne-Farrar and Josh Lerner estimated in a recent study, for instance, that the most “complete” modern pools contain eighty-nine percent of the patents that a licensee might need.⁴⁸ The least complete pools, they estimated, contained as few as ten percent of the necessary patent rights. They also estimated that “most pools contain roughly one-third of the eligible firms.”⁴⁹ In 2015, Justus Baron and Tim Pohlmann built upon this work by examining even more pools

44. See generally Merges & Mattioli, *supra* note 15. Our study was prompted in part by recent calls for greater antitrust regulation of pools. See, e.g., Steven C. Carlson, *Patent Pools and the Antitrust Dilemma*, 16 YALE J. ON REG. 359, 383 (1999) (“[T]he DOJ and the FTC should not adopt a per se rule of legality for the pooling of blocking patents, and that they must carefully stipulate the permissible bounds of those pools deemed procompetitive”); Scott Sher, Jonathan Lutinski & Bradley Tennis, *The Role of Antitrust in Evaluating the Competitive Impact of Patent Pooling Arrangements*, 13 SEDONA CONF. J. 111, 112 (2012) (“[A]ntitrust enforcement can and should take a more central role in the evaluation of the competitive effects of mass marketed patent pools containing thousands of separate and likely competing patents”).

45. See Merges & Mattioli, *supra* note 15, at 319–24.

46. *Id.* at 327–38.

47. See Anne Layne-Farrar & Josh Lerner, *To Join or Not to Join: Examining Patent Pool Participation and Rent Sharing Rules*, 29 INT’L J. INDUS. ORG. 294, 299 (2011).

48. See *id.*

49. *Id.* at 298.

and reported consistent findings.⁵⁰ Most patent pools, it would seem, are not grand coalitions.⁵¹

One reason why patent pools are incomplete in this sense is that they often form through a gradual process. Groups of technology companies usually collaborate to design technology standards.⁵² This work is often mediated by standard-setting organizations (SSOs).⁵³ SSOs often require collaborators to promise that they will declare any standard-essential patents (SEPs) that they hold and to license any such patents under “fair, reasonable and non-discriminatory” (FRAND) terms.⁵⁴ This standard-setting process usually comes before any patent pool forms. Only later, once a draft of the standard has been finalized, might some of the collaborators work toward forming a pool.⁵⁵ Typically, the organizers of such a pool issue a public call for patents and hire an independent expert to evaluate whether any declared patents are essential to the standard. This two-step process—standard-setting followed by pool formation—is a hallmark of pools designed around modern technology standards.⁵⁶

Layne-Farrar and Lerner cleverly estimated the participation rates in modern standards-based patent pools by comparing the numbers of patents included in those pools with the total numbers of patents declared (by their owners) to be essential to those pools.⁵⁷ They explained that the difference between these numbers could be the result of deliberate, calculated outsider behavior, or simply by disagreements concerning essentiality: “for those firms that *do* join [pools],” they wrote, “their patents are subject to an independent

50. See Justus Baron & Tim Pohlmann, *The Effect of Patent Pools on Patenting and Innovation – Evidence from Contemporary Technology Standards* 13–16 (Feb. 2, 2015) (unpublished manuscript), http://www.law.northwestern.edu/research-faculty/searcenter/innovationeconomics/documents/Baron_Pohlmann_effect_of_patents.pdf [<https://perma.cc/RJ9-V8YJ>].

51. See Gilbert, *supra* note 36, at 17 (“The grand coalition is the set of all the relevant players.”).

52. See generally Jorge L. Contreras, *Patents, Technical Standards and Standards-Setting Organizations: A Survey of the Empirical, Legal and Economics Literature*, in 2 RESEARCH HANDBOOK ON THE ECONOMICS OF INTELLECTUAL PROPERTY LAW: ANALYTICAL METHODS (Peter S. Menell et al. eds., forthcoming 2018) (providing an overview of interoperability standards and standards setting organizations).

53. *Id.* at 3 (working version).

54. *Id.* at 17 (working version).

55. See Jorge L. Contreras, *When a Stranger Calls: Standards Outsiders and Unencumbered Patents*, 12 J. COMPETITION L. & ECON. 507, 510–12 (2016).

56. Since the 1850s, patent pools have formed differently in many industries. Some have been collective solutions to litigation among patent holders, while others have been in response to pressure exerted by the federal government. See Mattioli, *supra* note 14, at 119–47.

57. Layne-Farrar & Lerner, *supra* note 47, at 297–301.

review for essentiality and not all patents declared as essential to a standard are actually found to be so.”⁵⁸ On its own, this evidence does not reveal whether the apparent lack of coverage in modern pools is the result of strategic outsider behavior or simply disagreements between patent holders and evaluators about essentiality.

But then Layne-Farrar and Lerner investigated patent pool participation more deeply. They examined whether patent holders were more likely to seek membership in patent pools that stood to compensate them relatively well.⁵⁹ Patent pools compensate their members by divvying-up royalties paid to the pool by licensees according to simple formulas.⁶⁰ Most commonly, these formulas are based upon *pro-rata* or *per-capita* divisions.⁶¹ This “rough and ready” approach to royalty sharing is attractive to many patent holders because it makes licensing simple, certain, and enables a volume of licensing that would otherwise be difficult and costly.⁶² Layne-Farrar and Lerner found that firms that possibly owned essential patents were less likely to seek participation in pools with royalty-division rules that stood to undercompensate them.⁶³ This finding, they explained, is suggestive of a deliberate outsider behavior rather than a disagreement over essentiality.⁶⁴ The authors did not conclude, however, that this kind of imperfect cooperation is a practical problem for pools.

1. *The Concerned View of Outsiders*

To understand why outsider behavior concerns some scholars, it is helpful to introduce two intertwined concepts: *holdouts* and *the complements problem*.⁶⁵ Hold-out situations often arise when a prospective property buyer or licensee

58. *Id.* at 298.

59. *Id.*

60. See Mattioli, *supra* note 12, at 439–55, 463 (cataloging royalty division and apportionment in historical and present-day pools).

61. *Id.*

62. *Id.* at 446 (referring to this as a “rough and ready” approach).

63. See Layne-Farrar & Lerner, *supra* note 47, at 296; see also Peter Bright, *New Patent Group Threatens to Derail 4K HEVC Video Streaming*, ARS TECHNICA (July 23, 2015, 9:55 PM), <http://arstechnica.com/tech-policy/2015/07/new-patent-group-threatens-to-derail-4-hevc-video-streaming/> [<https://perma.cc/EU4Q-Y76A>] (“If those companies are unhappy with MPEG LA’s terms, they don’t have to participate. It appears so far that at least five companies have decided to do just that: HEVC Advance claims General Electric, Technicolor, Dolby, Philips, and Mitsubishi Electric as members.”).

64. *Id.*

65. The first discussion of this problem is typically credited to the French mathematician AUGUSTIN COURNOT. See AUGUSTIN COURNOT, RESEARCHES INTO THE MATHEMATICAL PRINCIPLES OF THE THEORY OF WEALTH 103–04 (Nathaniel T. Bacon trans., 2d ed. 1971) (1838) (explaining the problem).

needs to strike deals with many individual property owners. A canonical example is the development of a shopping mall that will sit where a set of individually-owned lots exist.⁶⁶ Upon learning that his or her rights are essential to the developer's plan, each property owner has an incentive to drive a hard bargain.⁶⁷ Trouble arises, however, if the owners of these complementary property rights individually demand prices that lead to an unworkable aggregate for the prospective buyer.⁶⁸ If one or more property owners demand royalties that are high enough, no deals will be made, rendering all parties worse off.⁶⁹ This is the complements problem.

In a 1999 article in the journal *Science*, Michael Heller and Rebecca Eisenberg argued that a similar dynamic may play out in patent licensing markets—i.e., that a single patent holder aware that it can block access to a necessary technology could hold out for high royalties.⁷⁰ If multiple patent holders behave in this way, with no regard for their impact on the overall cost for would-be licensees, the technology may become too costly to license. They famously termed this outcome “The Tragedy of the Anticommons.”⁷¹ The authors acknowledged, however, that patent pools could overcome this problem.⁷² Robert Merges later developed this point into a landmark publication that offered some optimism: patent pools themselves are the evidence, Merges argued, of the power of private actors to wisely overcome holdout situations and the related complements problem.⁷³

Outsiders (as the term is used in this Article) are like traditional holdouts, but they imply some unique dynamics. Like the holdout, the outsider pressures a buyer or licensor for supracompetitive rates. Unlike the holdout, however, the outsider can also lean upon a set of insiders—i.e., a group of complementary rights holders. The outsider seeks to bargain in the shadow of

66. See, e.g., Richard McGregor & Yu Sun, *China's 'Nail House' Floors Developers*, FIN. TIMES, Mar. 27, 2007, at 6 (offering a real-life example of this holdout behavior).

67. See Thomas F. Cotter, *Patent Holdup, Patent Remedies, and Antitrust Responses*, 34 J. CORP. L. 1151, 1160 (2009) (discussing the holdout or holdup dilemma); Shapiro, *supra* note 14, at 124–29 (same).

68. Shapiro, *supra* note 14, at 125

69. *Cf. id.*

70. Heller & Eisenberg, *supra* note 14, at 698. Arti Rai has also written important foundational commentary on modern patent pools in the biopharmaceutical industry and in the consumer technology industry—including the pools studied in this Article. See Arti K. Rai, *Fostering Cumulative Innovation in the Biopharmaceutical Industry: The Role of Patents and Antitrust*, 16 BERKELEY TECH. L.J. 813, 848 (2001) (“To be sure, the MPEG-2 and DVD patent pools represent something of a high-water mark of procompetitiveness in a patent pool.”).

71. Heller & Eisenberg, *supra* note 14, at 698.

72. See *id.* at 701.

73. See Merges, *Contracting into Liability Rules*, *supra* note 12, at 1319.

this cooperative group, trading off its efficiencies.⁷⁴ In doing so, the outsider can theoretically not only demand high rates from licensees, but also exert pressure on the insiders by demanding a larger share of the pie in exchange for its cooperation.⁷⁵

Scholarly concerns about patent pool outsiders first surfaced in a paper written by Reiko Aoki and Sadao Nagaoka, published in 2005. The paper examined the factors that might lead patent holders in different industries to become pool outsiders.⁷⁶ The authors presented an economic model that explained how outsiders who negotiate in the shadow of established patent pools could, under some circumstances, demand higher royalties than the pool would deliver. The outsider can free-ride, they posited, off the efficiencies and certainty of licensing enabled by the pool.⁷⁷ Their model suggested, however, that this will usually tend to happen when the number of essential patent holders is large.⁷⁸ In settings where few patent holders operate, they predicted that a “grand coalition” is possible.⁷⁹ Considering the large numbers of

74. François Lévêque & Yann Ménière, *Technology Standards, Patents and Antitrust*, 9 COMPETITION & REG. NETWORK INDUSTRIES 29, 34 (2008) (“Still, some patent owners may prefer not to participate in the patent pool so as to take advantage of the collective self-discipline accepted by those who did join the pool. This hold out problem arises basically because an essential patent owner can always charge a higher price if it manages to set its price after the others.”). For the foundational discussion of the “bargaining of the shadow” concept, see generally, Robert Cooter et al., *Bargaining in the Shadow of the Law: A Testable Model of Strategic Behavior*, 11 J. LEGAL STUD. 225 (1982).

75. In other words, this expanding body of scholarship suggests that cooperative failures not only lead to suboptimal licensing, but also that at least some patent holders waste capital in ill-fated efforts to prevent that very result. See also Steffen Brenner, *Optimal Formation Rules for Patent Pools*, 40 ECON. THEORY 373, 374 (2009) (discussing the outsider problem as it affects the welfare-enhancing aspects of patent pools); Gilbert, *supra* note 36, at 17–18 (discussing the factors that might make joining a pool more or less compelling to an individual patentee); Daniel Quint, *Pooling with Essential and Nonessential Patents*, 6 AM. ECON. J. MICROECONOMICS 23, 34 (2013) (noting that the outsider problem “creates a free rider problem which may prevent pools from reaching their optimal size”); Gastón Llanes & Joaquín Poblete, *Ex Ante Agreements in Standard Setting and Patent Pool Formation*, 23 J. ECON. & MGMT. STRATEGY 50, 50 (2014) (studying the effects of “pool-formation rules on technology choice, prices, and welfare”).

76. See Aoki & Nagaoka, *supra* note 11, at 3. The authors explained that “[t]he breakdown of an integrated patent pool,” caused either by an outsider, or by the splintering of the pool into multiple licensing groups, “not only raises the total price to be paid by the licensees but also reduces the joint profit of the patentees.” *Id.*

77. See *id.* at 8; see also Mattioli, *supra* note 12, at 439–51 (indicating that patent pools allocate royalties to their members through formulas agreed upon when the pool is created).

78. See Aoki & Nagaoka, *supra* note 11, at 21 (“[T]he emergence of an outsider is inevitable [because] . . . a firm can gain by becoming an outsider and [this] gain increases as the coalition of the other firms expands.”).

79. *Id.* at 21 (“[A] grand coalition can be implemented only if the number of essential patent holders (n) is small.”).

essential patents in modern standards pools, the authors concluded, “there is indeed a risk of the tragedy of anti-commons.”⁸⁰

In a 2003 California Law Review article, Michael R. Franzinger expressed similar concerns relating to a patent pool designed to cover 3G wireless technologies.⁸¹ The wireless giant, Qualcomm, Franzinger explained, was vocal in its reluctance to join the pool. Franzinger posited that this may have been because Qualcomm drew its revenues primarily from licensing rather than manufacturing.⁸² “Especially for a nonmanufacturing patent holder who only wishes to license out its technology and not to obtain reciprocal licenses from others,” he wrote, “there would seem to be no good reason to join the Platform.”⁸³ Franzinger added, “[t]he lack of full industry-wide participation may dilute the competitive benefits of [a patent pool] more than it dilutes its dangers,” and concluded that the risk of “capture” presented by patent pool outsiders is significant and deserving of policy intervention.⁸⁴

In a 2010 article, the esteemed economist Richard Gilbert observed that “patentees are not compelled to negotiate with other patentees” to address a collective negative externality.⁸⁵ Gilbert explained that the more a pool thrives, the greater is there a rational impulse for members to defect.⁸⁶ In the context of patent pools, Gilbert wrote:

The more the pool succeeds in lowering royalties and avoiding transaction costs, the greater is the benefit from independent licensing of an essential patent. The incentive to leave the pool (or not join in the first place) is analogous to the incentive to defect from a cartel. By restricting output and raising prices, harmful cartels make it profitable for a firm to act as an independent competitor.⁸⁷

Gilbert analyzed the outsider problem through the economic theory of the core—a framework that examines the ability of players in a given economic setting to form beneficial coalitions.⁸⁸ “In the patent example,” he explained, “the core exists if every patentee prefers its payoff when part of a pool that consists of all patentees to the payoff it could get in any different coalition of

80. *Id.* at 22.

81. Michael R. Franzinger, *Latent Dangers in a Patent Pool: The European Commission’s Approval of the 3G Wireless Technology Licensing Agreements*, 91 CALIF. L. REV. 1693, 1706 (2003).

82. *See id.*

83. *Id.*

84. *Id.*; *see id.* at 1727.

85. Gilbert, *supra* note 36, at 17 (“The grand coalition is the set of all the relevant players.”).

86. *Id.* at 16–8.

87. *Id.*

88. *Id.* at 18.

patentees.”⁸⁹ Gilbert further added that “[p]atent owners that choose to remain outside a pool can unravel the benefits from pooling by interfering with one-stop shopping and by demanding high royalties.”⁹⁰

It is helpful to synthesize these concerns into a coherent picture. One concern appears to be that licensees will pay more in settings where a sole licensor operates outside of a pool than they would pay if the same patent holder had joined the pool.⁹¹ If this cost difference is great, it might shut some would-be licensees out of the market. A related concern has to do with the effect that outsiders have on the overall cohesion of the pool. If every member of a pool acts on a rational impulse to “go it alone,” the group will splinter apart, setting the stage for an anticommons.

Although there have been no empirical studies of the impact of patent pool outsiders, Jorge Contreras’ recent study of patent infringement lawsuits brought by “standards outsiders” helps illuminate this discussion.⁹² Contreras was interested in patent holders unencumbered by FRAND obligations. He identified lawsuits where such “standards outsiders” brought suits against technology producers.⁹³ Contreras’ research goal was to see whether “[the standards outsiders] could potentially seek rents in excess of the rates received by [insiders].”⁹⁴ Contreras found that suits brought by outsiders make up an appreciable proportion of all assertions of standard-essential patents.⁹⁵ He also found that the companies that bring these suits most often are so-called nonpracticing entities.⁹⁶ These conclusions are concerning, but they leave open the question of what impact, if any, patent pool outsiders have on the efficiencies pools offer.

89. *Id.*

90. *Id.* at 28.

91. It is helpful to distinguish this concern from the concern that royalty-free cross-licenses between pool members can give them an unfair advantage over licensees. Kenneth Flamm argued that this advantage became unfair in the DVD landscape as the price of manufacturing the technology dropped: “Within a few short years, however, the royalties charged by the DVD patent pools evolved into truly significant sums relative to the total cost of manufacturing optical disk drives (ODDs)—indeed they now account for the majority of manufacturing cost for a potential entrant.” Kenneth Flamm, *A Tale of Two Standards: Patent Pools and Innovation in the Optical Disk Drive Industry* 20 (Nat’l Bureau of Econ. Research, Working Paper No. 18931, 2013), <http://www.nber.org/papers/w18931.pdf> [<https://perma.cc/Z42Q-2RX3>]. This criticism is not really about the outsider problem, however.

92. See Contreras, *supra* note 55.

93. *Id.* at 507.

94. *Id.* at 520.

95. *Id.* at 535.

96. *Id.* at 518–19.

Industry stakeholders and market analysts are often concerned by outsiders as well. In 2015, for instance, industry commentators warned that the existence of two 4K video patent pools “threatened to derail” the future of streaming videos by increasing the cost of licensing of the underlying technology.⁹⁷ In 2012, when Nokia, Apple, and Google withdrew from patent pooling efforts related to the LTE wireless data standard used by smartphones, similar predictions were reported in the Wall Street Journal.⁹⁸ A few years earlier, industry analysts made similar comments about the 3G wireless data and MPEG-2 video patent pools, each of which did not include important patent holders.⁹⁹

2. *The Sanguine View of Outsiders*

Antitrust authorities have assumed that patent pool outsiders are not a problem. Their assumption is simply that some pooling is more helpful than none at all.¹⁰⁰ This optimistic view is supported by ample anecdotal evidence:

97. Stephen Shankland, *Next-gen High-res Video Faces New Fees and Uncertainty*, CNET (Mar. 26, 2015, 6:40 PM), <http://www.cnet.com/news/patent-group-raises-new-fees-uncertainty-for-4k-video/> [<https://perma.cc/T3RK-ZZ7N>]. (“‘[The introduction of HEVC Advance] creates confusion in the market,’ especially given MPEG LA’s pool of patents from 27 different patent holders, said Frost & Sullivan analyst Dan Rayburn. ‘They put out a press release that scares a lot of content owners, and then won’t give any details . . . I’ve got content owners saying this is bad for my business.’”).

98. See Don Clark, *Plan to Pool LTE Patents Takes Shape*, WALL ST. J. (Oct. 3, 2012, 8:01 AM), <https://blogs.wsj.com/digits/2012/10/03/plan-to-pool-lte-patents-takes-shape/> [<https://perma.cc/L2GW-G79E>] (acknowledging that some companies tend to act independently when it comes to patent matters).

99. See Franzinger, *supra* note 81, at 1706. (“The lack of full industry-wide participation may dilute the competitive benefits of the Platform more than it dilutes its dangers.”); Vikrant Narayan Vasudeva, *Patent Valuation and License Fee Determination in Context of Patent Pools*, CTR. FOR INTERNET & SOC’Y (July 9, 2014), <https://cis-india.org/a2k/blogs/patent-valuation-and-license-fee-determination-in-context-of-patent-pools> [<https://perma.cc/4895-W3U6>] (“Correspondingly, if the patent pool does not contain all the patents it cannot curtail royalty stacking issues for the users. For example, Alcatel-Lucent pursued infringement claims for patents that it alleged covered the MPEG-2 standard and were not in the pool.”).

100. See, e.g., Letter from Joel Klein, Assistant Att’y Gen., U.S. Dep’t of Justice, to Garrard R. Beeney, Esq., Sullivan & Cromwell 13 n.58 (Dec. 16, 1998), <https://www.justice.gov/sites/default/files/atr/legacy/2006/04/27/2121.pdf> [<https://perma.cc/EJ3W-5JH7>] [hereinafter DVD Business Review Letter] (“Transaction costs to licensees would almost certainly be somewhat lower if these later patents were included in the pool, instead of being subject to separate negotiations. However, the fact that this pool might not enable the realization of all potential efficiencies of pooling patents in this area does not mean that the efficiencies that it does create are insubstantial or that the arrangement is anticompetitive or unlawful.”); RFID Business Review Letter, *supra* note 23, at 8 (proposing that a pool will yield cognizable efficiencies, although those efficiencies may not be as great as they would be if the pool contained all essential patents); Gilbert, *supra* note 36, at 26 (“Nonetheless, even partial pools that do not include all patents that are necessary to make or use a product offer

as mentioned earlier, many important industries appear to have flourished due to patent pools. If outsider behavior was truly a problem, one would expect to see far fewer successful pools, as well as lower commercialization and higher prices of the technologies around which they are organized.

In a 2006 paper, Douglas Lichtman suggested why this might be. He made the important point that outsiders could be companies that are known *before* a technology is in widespread use or *after* the fact.¹⁰¹ In the former case, an outsider theoretically would possess only the power to demand royalties that reflect the marginal value of its patents. This would be because, if an outsider's demands are viewed as excessive by prospective licensees (which may include pool members), given enough time, the industry can simply adopt a different technology in place of the one hold-out. Lichtman theorized that patent holders that assert themselves after a technology is in widespread use, meanwhile, may ironically be in a poor position if there are very many of them. Just as a creditor can only receive a smaller share of the pie if it is one of many, Lichtman posited, in a market that can only pay a limited maximum rate, each of many outside licensors can only have a weak leverage.¹⁰² Lichtman believed that licensees have more power and that patent holders are more farsighted than the pessimists have guessed. These predictions cast doubt on the outsider concern. As Lichtman explained, the risk of being one of many holdouts fosters "less of an incentive for a firm to strategically delay in the hopes of being a patent holdout, and less of an incentive for an accidental patent holdout to actually bring suit."¹⁰³

Another possibility is that pools set a practical baseline for independent licensors. A recent dispute between Microsoft and Motorola suggests this is so. In *Microsoft Corp. v. Motorola, Inc.*, the Ninth Circuit instructed that a patent pool may serve as a useful data point in determining a "reasonable" rate under a FRAND obligation.¹⁰⁴ Jonathan Barnett posited that multiple complementary patent licensors may "signal" royalty rates to one another,

considerable savings in transaction costs and can mitigate royalty stacking compared to separate licensing with independent patentees."); Mark A. Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 TEX. L. REV. 1991, 2014–15 (2007) ("Such a patent holder might well maximize its revenues by staying out of a proposed patent pool and asserting its patent rights independently, unless it believes that its failure to join the pool will undermine the formation of the pool and thus seriously hinder sales of the product in question.").

101. See Douglas G. Lichtman, *Patent Holdouts and the Standard Setting Process* 1–3 (Univ. of Chi. John M. Olin Law & Econ. Working Paper, Paper No. 292, 2006).

102. See *id.* at 6–7.

103. *Id.* at 6.

104. See *Microsoft Corp. v. Motorola, Inc.*, 795 F.3d 1024, 1043 (9th Cir. 2015) ("Motorola provided no evidence that its patents were more valuable than the other patents in the pool.").

leading to an aggregate cost that is workable.¹⁰⁵ As the study presented in Part III of this Article shows, Barnett is correct.

In addition, patent owners do not always sue unlicensed users. Herbert Hovenkamp and Eric Hovenkamp suggest that a licensee will not be “meaningfully blocked as a matter of fact” if, “for example, . . . there is a widespread belief that a blocking patent is invalid, such that competitors are willing to practice the blocked technology without a license notwithstanding the risk of an infringement suit.”¹⁰⁶ This accords with Rebecca Eisenberg’s observation—which has been echoed by other scholars—that many patented technologies are used without permission with no legal consequences for the infringer.¹⁰⁷ Because of this, Eisenberg notes, the effective reach of a patent may fall short of its nominal reach.¹⁰⁸ This reasoning suggests that the same may be true for patent pools: a pool that does not contain all patents that relate to a technology may nonetheless be *effectively* complete if the outsiders permit the unlicensed use of their patents.

On one side of this debate, economic theory urges greater concern over patent pool outsiders; on the other side, the long-held intuition of regulators is that these independent patent holders do not meaningfully detract from the transaction costs that pools mitigate. If the theorists have it right, then regulators may wish to rethink their long-held assumptions; if, on the other hand, regulators are correct that outsiders dampen the benefits of patent pools, then academic debate on this subject could be meaningfully advanced. The next Part presents the results of an original study that adds new empirical insights to this debate.

105. See Jonathan Barnett, *From Patent Thickets to Patent Networks: The Legal Infrastructure of the Digital Economy*, 55 JURIMETRICS 1, 41–42 (2014).

106. HERBERT HOVENKAMP, MARK JANIS, MARK LEMLEY & CHRISTOPHER R. LESLIE, IP AND ANTITRUST: AN ANALYSIS OF ANTITRUST PRINCIPLES APPLIED TO INTELLECTUAL PROPERTY LAW § 34.04[C] at 34-8 (3d ed. 2016).

107. See Jonathan M. Barnett, *Has the Academy Led Patent Law Astray?*, 32 BERKELEY TECH L.J. (forthcoming 2017) (arguing that unlicensed infringing uses are extremely common); David J. Teece, *The “Tragedy of the Anticommons” Fallacy: A Law and Economics Analysis of Patent Thickets and FRAND Licensing*, 32 BERKELEY TECH. L.J. (forthcoming 2017) (arguing that uncompensated, infringing uses are net more harmful to innovation than patent thickets); Rebecca Eisenberg, *Patent Costs and Unlicensed Use of Patented Inventions*, 78 U. CHI. L. REV. 53, 53–54 (2011) (“Empirical work suggests that unlicensed use of patented inventions is common in research Unlicensed use is likely pervasive in other settings as well, including commercial production.”).

108. See Eisenberg, *supra* note 107, at 55–56.

III. AN ETHNOGRAPHIC STUDY OF PATENT POOL OUTSIDERS

This Part presents a study of patent pool outsiders—i.e., episodes where essential patent holders have declined to join pools and instead licensed independently.

A. METHODOLOGY

The methodology followed here was deeply influenced by the work of Nobelist Elinor Ostrom, who famously developed the Institutional Analysis and Design (IAD) framework. Using this approach, which entails defining broad categories of inquiry, Ostrom and the many scholars she inspired have shed light on how groups manage shared resources (including property rights) in a variety of settings.¹⁰⁹ Katherine Strandburg, Brett Frischmann, and Michael Madison have recently adapted the IAD framework to the study of “knowledge commons,” such as patent pools.¹¹⁰ Inspired and informed by this body of work, this Article adopts a similar ethnographic approach.¹¹¹

This study analyzes the following research question: “Do outsiders (independent licensors) impose significant costs on licensees or otherwise undermine the transaction costs conserved by patent pools?” I focused my research on the following research topics¹¹²: (1) the technological, industrial, and social contexts in which outsider episodes occurred; (2) the patents involved, including their numbers and their relationships to the patents in pools; (3) the firms and institutions involved; (4) the motivations and goals of the licensors and pool administrators involved; (5) the internal governance

109. See generally ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 182–85 (1990). For an example of an ethnographic approach applied to study outsiders outside of patent settings, see generally Cole, *supra* note 2 (examining how outsider nations that refused to join the Kyoto Protocol affected the underlying goals of the federation of countries that did join). Surprisingly, outsiders in that setting not only failed to weaken, but in fact strengthened, coalitions of rights-holders.

110. See generally Peter B. Meyer, *An Inventive Commons: Shared Sources of the Airplane and Its Industry*, in GOVERNING KNOWLEDGE COMMONS 341 (Brett M. Frischmann, Michael J. Madison & Katherine J. Strandburg eds., 2014).

111. The methodology carried out borrowed heavily from the IAD framework but did not formally adhere to that framework in every respect. See Michael Mattioli, *The Data-Pooling Problem*, 32 BERKELEY TECH. L.J. 179, 224 (2017) (describing an analogous targeted application of the IAD framework). More specifically, aspects of the IAD framework that were not relevant to the central question under examination were not employed.

112. Brett M. Frischmann et al., *Governing Knowledge Commons*, in GOVERNING KNOWLEDGE COMMONS 1, 20 (Brett M. Frischmann, Michael J. Madison & Katherine J. Strandburg eds., 2014).

rules of the pools and outside licensors involved; (6) outcomes, with a focus on costs and benefits.

This work began with a broad literature review. To learn about the topic and to identify potential case studies and research study subjects, I searched through newspaper and industry press archives for well-documented episodes of patent pool outsiders. Because this work revealed several episodes that involved litigation, I carefully studied lawsuits by reviewing court decisions, docket filings, and corporate press releases, such as announcements of settlements. Because the DOJ reviewed the pools examined, this study gathered helpful details from publicly available letters exchanged between pool organizers and the Antitrust Division of the DOJ.¹¹³ I also gathered critical information about pool composition (patents, membership, and licensees) from the websites of patent pool administrators. Archived copies of these same webpages revealed pool membership data from earlier points in time.¹¹⁴ In some cases, publicly available annual reports to shareholders were reviewed as well.

With a preliminary record assembled, I sought to construct a deeper and richer understanding by interviewing individuals directly involved with selected outsider episodes. I contacted and interviewed executives and lawyers who work for the largest patent pool administrators in the United States. I then interviewed executives and counsel at large technology companies, some of which were members of pools, and some of which were outsiders of prominent pools.

All interviews were conducted by telephone and email in a semi-structured fashion and focused on a set of interview questions that I shared with the individuals beforehand. The questions were divided into two lines of inquiry: the impact of outsider behavior on patent pools generally, and questions pertaining to specific case studies. Most conversations led to follow-up emails and phone conversations. In the interest of clarity, the findings are reported here in three sub-parts: a set of general observations followed by two deep case studies.

A note on the selection of case studies: there are many episodes of outsider behavior that can be analyzed. This study proceeded on the premise that depth would be more helpful than breadth. Rather than cataloging as many outsider episodes as possible, the goal was instead to provide deep and nuanced

113. See *Business Review Letters and Request Letters*, U.S. DEP'T OF JUSTICE, <https://www.justice.gov/atr/business-review-letters-and-request-letters> [https://perma.cc/RL84-WSWG] (last updated Dec. 27, 2017).

114. Historical copies of these pages were gathered from the Internet Archive. See *About the Internet Archive*, INTERNET ARCHIVE, <https://archive.org/about/> [https://perma.cc/TU5V-7PEB] (last visited Mar. 11, 2018).

portraits of this behavior. The first two modern-day patent pools, covering MPEG-2 video and DVD, were selected because they revealed a rich variety of dynamics and because they are related to one another, as explained in the discussion that follows. Research subjects opined that these two episodes offer lessons that are broadly applicable. Research subjects also offered high-level insights on outsider behavior, generally. This information is presented first.

Relatedly, although great efforts were made to avoid bias, it is possible that selection bias is present. Selection bias is a fundamental challenge in nearly all ethnographic work, and the challenge is heightened where the sample size—i.e., the number of cases observed—is small, as it is here.¹¹⁵ To minimize this risk, I analyzed as many relevant episodes as I could find and based my “general” category of questions on what those episodes appeared to reveal. Research subjects explained that the two selected case studies illustrate important dynamics between outsiders and patent pools. It is possible that the individuals who agreed to be interviewed for this study may, by coincidence, happen to share similar subjective opinions. To minimize the odds of this, the interviews include a range of experts on different sides of the outsider issue—i.e., outsiders, insiders, and pool administrators—however.

An additional challenge is the fact that the only episodes that could be explored deeply were those in which patent pools had successfully taken form. At least one licensor speculated that a “critical mass” of licensors must agree to join a patent pool for any cooperation to take place at all. Because there is little to no available information on point, it is very difficult to examine pools that might have formed but did not. Fortunately, however, this study can comfortably leave such episodes out of the analysis: the purpose of this Article is to offer insights to antitrust regulators who are tasked with examining patent pools that have necessarily gathered sufficient critical mass.

B. THE UNAPPRECIATED INFLUENCE OF POOLS

This section describes general observations that interview subjects shared about patent pools and outsiders who decide, for various reasons, not to join a pool. The two case studies that follow this discussion illustrate the insights summarized here.

As a threshold matter, interview subjects explained that it is difficult to say with certainty if any patent pool contains “all” of the necessary patents involved. “There’s no way to know whether you have all of the patents in a

115. See AMY R. POTEETE, MARCO A. JANSSEN & ELINOR OSTROM, WORKING TOGETHER 36 (2010) (“Small samples present two serious limitations: selection bias and indeterminacy. A sample is biased if the cases observed do not represent variation on the dependent or independent variable accurately.”).

pool,” one subject commented.¹¹⁶ He added, “there might be unknown patent holders at the time of a pool’s formation.”¹¹⁷ Another subject stated that it is almost “inevitable” that there are one or more independent or outside patent holders.¹¹⁸ Some are, this subject explained, nonpracticing entities that own patents that “just happen, by coincidence, to read on the standard to which the pool relates.”¹¹⁹

These observations capture a fundamental insight: patent pooling is not neatly analogous to real property assembly, such as the canonical land development example discussed in Part I. Unlike the land developer who can know with certainty the underlying property rights that she must gather before breaking ground, a technology manufacturer can never be entirely sure of every possible patent that might read on its product. This is because the boundaries of patent rights are inherently less certain than those of real property.¹²⁰ Relatedly, the validity (and hence, the enforceability) of the patents identified is generally less certain than the rights of a property owner.¹²¹ The operative question for manufacturers, then, might not be whether a pool contains “all” of the relevant patents in existence, but rather, whether the pool helps licensees obtain permission from the companies most likely to sue them for infringement. Stated differently, the technical or *nominal coverage* of a pool may be less important than its *effective coverage*.

Moving beyond this threshold observation, the most important insight shared by research subjects is that patent pools significantly influence the royalty rates that outsiders can ask for and receive. By publishing their rates, patent pools signal the value of the portfolios of patents they offer. This gives licensees a basis to negotiate rates for other essential patents outside of the pool. As one subject stated, “there is no doubt that the royalties asked by a major pool influence the royalties asked by other patent holders.”¹²² Another

116. Telephone Interview with Larry Horn, President & CEO, and Bill Geary, Vice President of Bus. Dev., MPEG LA, LLC (Feb. 23, 2017) [hereinafter Telephone Interview with Horn & Geary] (on file with author).

117. *Id.*

118. Telephone Interview with Ruud Peters, Exec. Vice President & Advisor, Koninklijke Philips N.V. (July 15, 2017) (on file with author).

119. *Id.*

120. Real property is defined by geographic coordinates. By contrast, the metes and bounds of patents are defined by claim language, which is inherently more subject to interpretation and validity challenges. See Clark D. Asay, *The Informational Value of Patents*, 31 BERKELEY TECH. L.J. 259, 270 (2016) (discussing this common analogy).

121. David J. Teece, *The “Tragedy of the Anticommons” Fallacy: A Law and Economics Analysis of Patent Thickets and FRAND Licensing*, 32 BERKELEY TECH. L.J. 1489, 1504 (2016) (discussing the impact of uncertainty with respect to validity on damages calculations).

122. Email from Subject #5 to author (July 11, 2017) (on file with author).

explained that the royalty rate offered by the pool not only limits the power of the outsider, but also “lowers negotiation costs by orders of magnitude for all licensing done in the shadow of the pool.”¹²³ Yet another subject added, “the patent pool sets a *de facto* market reference.”¹²⁴

A pool’s rate signals a ballpark sense of value. It would be a mistake to assume that a patent pool’s influence can be boiled down to a simple “per-patent” measure of value. One reason for this is that the composition of patent pools is dynamic. Old patents expire, new patents join, and all the while, the royalty rate charged by the pool does not rise or fall in response.¹²⁵ As a result, a simple per-patent calculation would problematically yield a frequently shifting baseline for outside negotiations. Alongside this problem is the fact that a single invention can spawn many patents. This is because inventions are often patented in different countries, and claims are sometimes split into divisionals.¹²⁶ Complicating licensing matters further, the same invention may not always be represented by the same number of patents in different countries. (A product that requires ten U.S. patent licenses to manufacture might require only seven German patent licenses, for instance.) This explains why the influence of patent pools on outside negotiations is not so simple as a per-patent pool rate.¹²⁷ Although some research subjects referred to the “per-patent” value of pools, further discussions clarified that this term was used imprecisely. A more helpful (but still imperfect) way to gauge a pool’s influence on outside negotiations at any point in time might be “per-

123. Email from Subject #4 to author (July 15, 2015) (on file with author).

124. Telephone Interview with Subject #3 (July 19, 2017) (on file with author).

125. Many pools, such as those administered by MPEG LA, drop their royalty rates over time, but this is not caused by the removal of patents. These decisions are made at the time of pool formation and discussions surrounding these decisions are typically confidential.

126. John R. Allison & Emerson H. Tiller, *The Business Method Patent Myth*, 18 BERKELEY TECH. L.J. 987, 1064 (2003) (describing “divisional” patent applications).

127. As one subject explained, “[p]atent pools are for the convenience of licensees in acquiring patent rights from multiple patent holders at a single rate in a single transaction as an alternative to negotiating separate license agreements, and the royalties [in our pools] are the same whether one or more patents is infringed/used . . . Similarly, neither do royalties increase or decrease based on the number of patents as licensors and patents are added to the pool or patent expire, and licensors would be unlikely to volunteer their patents for the benefit of licensees if they did. Instead, there is a royalty rate for a pool license based on striking a balance between what it takes to retain licensors and offer reasonable terms to licensees over the course of a license, and this concept is important for understanding a pool’s operation and success.” Email from Larry Horn, President & CEO, and Bill Geary, Vice President of Bus. Dev., MPEG LA, LLC to author (July 21, 2017) [hereinafter Email from Horn & Geary] (on file with author).

invention” or “per-patent-family” royalties—a higher number than a “per-patent” calculation would produce.¹²⁸

There are several reasons why patent pools can exert such an influence on negotiations. One explanation appears to be a widespread understanding that, if an outsider sued a pool licensee for patent infringement and won, under several common scenarios, a court would likely look to the patent pool as a reflection of the value of the outsider’s patent. The court would assume that, had the outsider been a participant in the standard-setting process, it would have likely made a FRAND commitment. *Microsoft v. Motorola*, discussed earlier, indicates that a court may look to a pool’s rates for an indication of whether an outsider’s demands are “reasonable,” such that they satisfy a FRAND obligation.¹²⁹ (Recall this decision also instructs that a FRAND commitment is a contract, removing the patent holder’s power to demand an injunction.)¹³⁰

A patent pool’s royalty rate could similarly affect an independent patent holder who is not subject to a FRAND commitment, however. As one subject explained:

The pool rate defines a ballpark figure for the per-patent royalty that you can ask. If you come in as an independent licensor and you demand a multiple of the per-patent royalty the pool is asking for [relative to the technology being licensed], then you will meet incredible resistance in the negotiations with the potential licensees. They will simply refuse to take a license. Then the licensor could only get companies licensed if it is prepared to sue. In that case, it needs to defend its case before court and it will need to show that its royalty is reasonable compared to what the pool is asking. That is costly, and takes a long time with an uncertain outcome. Most licensors don’t want to litigate each and every company and wait for years and years to get their money. So, they are forced to lower their royalties to a level that the market finds acceptable.¹³¹

128. A subject interviewed explained that such negotiations should “begin with the recognition that patent pools are for the convenience of licensees in acquiring patent rights from multiple patent holders at a single rate in a single transaction as an alternative to negotiating separate license agreements and the royalties are the same whether one or more patents is infringed/used.” Email from Horn & Geary, *supra* note 127.

129. See Susan Decker, *Ericsson Tries to Avoid Patent War by Publishing Rates for 5G*, BLOOMBERG (Mar. 17, 2017, 11:00 AM), www.bloomberg.com/news/articles/2017-03-17/ericsson-tries-to-avoid-patent-war-by-publishing-rates-for-5g [<https://perma.cc/TR8W-7JC8>].

130. *Microsoft Corp. v. Motorola, Inc.*, 696 F.3d 872, 877 (9th Cir. 2012) (“[B]ecause of the RAND licensing commitment, injunctive relief is an inappropriate remedy for infringement of standard-essential patents.”).

131. Telephone Interview with Ruud Peters, *supra* note 118.

Another subject made consistent comments, stating that, faced with a high royalty demand from an outsider, pool licensees may sometimes decide to “efficiently infringe” the patent, even if it is essential to a standard.¹³² The outsider can sue for infringement, that subject explained, but injunctions are difficult to obtain in these settings, and monetary awards are more common.¹³³ At this stage, explained the subject, it will be up to a court to determine the value of the infringed patents. Where might the court look? Common wisdom is that the pool is a likely source.¹³⁴

The situation is even more constrained for an outside patent holder that is also a technology manufacturer, a common situation. To operate, these patent holders should obtain licenses to the necessary patents. They may do so through the pool or by contacting the individual patent holders. As discussed earlier in this Article, some pools have historically required grant-back promises from licensees, obligating them to license any essential patent rights back to the pool. As one subject explained, “a patent holder who also manufactures products using the pool technology may be constrained by a grant-back provision if he must sign a license with the pool and will necessarily grant licenses based on the pool royalty level.”¹³⁵ Another subject commented, “an outsider could ask for very high royalties only if it does not have business exposure and so doesn’t need to become a licensee.”¹³⁶

Subjects explained that, even in pools without grant-back provisions, outside licensors who are also manufacturers may experience similar pressures. The reason lies in the simple fact that the independent must come to an agreement with the patent holders in the pool. “They will still need licenses from the pool licensors,” explained one subject:

These pool licensors will say to the independent, “I am a member of the pool. You are asking on a per-patent basis a multiple of what we are asking for our patents. So, either we go with my per-patent royalty or we take yours. If we go with yours, then you need to pay me your per-patent royalty for the use of my patents.”¹³⁷

An outside licensor in this position who asks for an unreasonably high rate, the subject explained, “is shooting itself in the foot.”¹³⁸

132. Telephone Interview with Subject #7 (Feb. 23, 2017) (on file with author).

133. *Id.*; see also *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 392–93 (2006) (instructing that, contrary to prior judicial practice, judges should not automatically issue injunctions upon finding patent infringement).

134. *Id.*

135. Email from Subject #5 to author, *supra* note 122.

136. Telephone Interview with Subject #3, *supra* note 124.

137. Telephone Interview with Ruud Peters, *supra* note 118.

138. Telephone Interview with Subject #3, *supra* note 124.

Remarkably, even outsiders who somehow succeed in getting licensees to agree to very high royalties do not always benefit in the end. The reason, according to some subjects, is the underreporting of sales. One research subject explained this through a hypothetical:

Let's say you have an independent that is commercially not active and assume that it asks for a relatively high royalty rate and that licensees agree in the end—because they want to avoid the cost of litigation—to take licenses. Normally, these licensees will be required to submit quarterly reports with the number of products they have sold in that quarter and thus the total royalty amount they have to pay. If licensees feel that the royalties they have to pay are too high, they may adjust their reported quantities, so that effectively their royalty rate comes within the range that they believe is more fair and reasonable.¹³⁹

Research subjects explained such underreporting “happens on a large scale,” even though it violates the contractual obligations of licensees under their license agreements.¹⁴⁰ In part, this is because underreporting is difficult and costly to detect. The subject quoted above explained that some licensees are very creative in masking underreporting. “Of course,” he stated, “the licensor can take measures, such as hiring an independent auditing firm to check the books of licensees, but that costs a lot of money and takes quite some time. In countries with different business practices, it's not always an easy job.”¹⁴¹

The foregoing explains why, as one subject opined, “an outsider might be able to negotiate a higher rate, but not that much higher.”¹⁴² The head of licensing at a large technology company that has historically operated inside and outside of some large pools commented, “if the per-patent rate is too different from the per-patent pool rate, potential licensees would rather fight in court than take the license.”¹⁴³ The subject added, “you may deviate in practice from the baseline by 30 or 40% but not by 300% for example.”¹⁴⁴

This leads to another observation: the existence of a patent pool not only sets a baseline for negotiations, but also eliminates the need for an outsider to

139. Telephone Interview with Ruud Peters, *supra* note 118.

140. *Id.*

141. *Id.*

142. *Id.*

143. Telephone Interview with Subject #3, *supra* note 124. Here, the term “per-patent” was used casually and imprecisely. The speaker was referring to per-patent-family or per-invention rates. *See supra* notes 124, 125, and accompanying text (discussing the problem with looking to per-patent rates).

144. Telephone Interview with Subject #3, *supra* note 124.

search for licensees and vice-versa—tasks that would contribute significantly to search costs in a world of one-to-one licenses. “We did a lot of their homework for them,” one pool administrator explained.¹⁴⁵ In summary, the very existence of the patent pool, in a sense, cuts down on both search costs and negotiation costs.¹⁴⁶ This can help licensees to get a clear picture of which patents are essential to license.

Interestingly, some research subjects explained that not all outsiders are holdouts seeking an economic advantage. Some are simply companies that have large, internal licensing staff who they wish to look out for by reserving work for them rather than going along with the pool.¹⁴⁷ The company might view both options as equal in terms of the bottom line and yet the option to go it alone can keep their people employed.

Finally, evidence gathered for this study shows that the decision to remain outside of a patent pool can raise the odds that a patent holder will need to litigate. As one research subject commented:

You may also have to litigate more, even though patent pools are litigating sometimes. If you are alone, you will have to do more litigation, so you may have more, you know, bad press articles about you because these companies may also play with the media. Certain companies would hate to have to litigate by themselves.¹⁴⁸

The MPEG-2 case study that follows provides a vivid example of this risk.

In summary, research subjects offered a surprising window into how patent pools limit the royalties that outside licensors can succeed in collecting. If the independent is a technology manufacturer, it typically must limit its demands if it wishes to use the patents in the pool (especially if it owes a contractual duty to grant-back). If the independent is not a licensee, the pool’s rate still is thought to be the basis in determining a reasonable royalty, either under a FRAND obligation or simply as a legal remedy. As one subject stated, “if the patent holder is not a pool licensee, his asking for high royalties will still be rejected by the licensees and his only solution for trying to get these will be litigation . . . with the associated risks.”¹⁴⁹ Finally, even an outsider that gets licensees to agree to a high rate faces the problem of underreporting and an increased risk of litigation. One subject summed the situation up well: “if they want to get some money, then they need to be moderate.”¹⁵⁰

145. Telephone Interview with Horn & Geary, *supra* note 116.

146. *Id.*

147. Telephone Interview with Subjects #12 and #13 (Feb. 23, 2017).

148. Telephone Interview with Subject #3, *supra* note 124.

149. Email from Subject #5 to author, *supra* note 122.

150. Telephone Interview with Ruud Peters, *supra* note 118.

C. OUTSIDE THE MPEG-2 PATENT POOL (CASE STUDY)

In the earliest days of filmmaking, about fifteen patents covered the technology needed to record and deliver movies to the public.¹⁵¹ These inventions covered flexible film, winding and spooling mechanisms, camera lenses, and related methods. In 1908, efforts to settle legal disputes between the two chief owners of these patents led to the formation of “The Motion Picture Patents Company”—the first of several patent pools that operated in the film industry of the early 20th century.¹⁵²

In the 1990s, the rise of digital video boosted not only the quality and transportability of movies but also the number of patent rights needed to play them. Many advances made it possible for celluloid and magnetic reels to be replaced by weightless computer instructions. One achievement, however, could be credited for the widespread adoption of digital video: the MPEG-2 video standard. Developed by (and named after) the Moving Picture Expert Group (MPEG) and a team of engineers and scientists from leading technology firms, MPEG-2 is a standardized way to describe motion, light, and sound through sequences of 1's and 0's. It is the language understood by DVD players, cable boxes, smart phones, digital cameras, online video providers, and video game consoles.

MPEG took form at a January 1988 meeting of the International Organization for Standardization (ISO) and held its first meeting in May of that year.¹⁵³ The group, which was open to any interested parties, held frequent meetings which were widely attended by delegates of leading technology companies. MPEG required its participants to pledge to license any patents they might own related to the standard under development at FRAND terms—a fact that would later have important bearing on one of its outsiders.¹⁵⁴ Over the course of a few years, at meetings held in Berlin, Australia, New York, Brussels, and Seoul, the MPEG-2 standard took form.

151. The chief patents were U.S. Patent Nos. 12,192; 12,037; 629,063; 578,185; 580,749; 586,953; 588,916; 673,992; 707,934; 722,382; 673,329; 744,251; 770,937; 771,280; 785,205; and 785,237. See INDUSTRIAL COMBINATIONS AND TRUSTS 259–65 (William S. Stevens ed., 1914) (listing the aforementioned patents).

152. See Ralph Cassady, Jr., *Monopoly in Motion Picture Production and Distribution: 1908–1915*, 32 S. CAL. L. REV. 325, 329 (1959); see also Jeanne Thomas, *The Decay of the Motion Picture Patents Company*, 10 CINEMA J. 34, 34 (1971) (indicating that The Motion Picture Patents Company formed in 1908 by the emergence of two factions of the film industry).

153. See Josh Lerner & Jean Tirole, *Public Policy Towards Patent Pools*, in 8 INNOVATION POLICY & THE ECONOMY 157, 174 (Adam B. Jaffe et al. eds., 2008) (“The standard was developed by the International Organization for Standardization (ISO) under the leadership of Leonardo Chiariglione, along with scientists and engineers from many universities and corporations.”).

154. See *id.* at 174–75.

The group produced a final draft in late 1994, and necessary stakeholders approved it in early 1995.¹⁵⁵

Although it took an ensemble of talented engineers to develop MPEG-2, the way the technology works is easy to grasp¹⁵⁶: movies, television, and other video are, of course, made up of sequences of still images. Thanks to a trick of human psychology, when viewed in rapid succession—twenty-four frames per second for film, and thirty frames per second for television video—the images appear to move.¹⁵⁷ Traditional analog movies create this illusion by storing thousands of images on film or magnetic tape and flashing them before the viewers' eyes.¹⁵⁸ As a practical matter, however, often only small areas of any frame in a sequence differ from the frame that immediately preceded it. Large swaths of a picture—the blue of a sky, or the green grass on a field, for instance—do not change. The information that matters most is what has changed between two successive frames. MPEG-2 cleverly takes advantage of this by formalizing a way to describe the portions of each image in a series that change from one frame to the next. The result is a phenomenally efficient method of compressing video, making for faster transfers over networks and more economical use of storage space on physical media.

Shortly following MPEG-2's completion in early 1995, one of the technology firms that helped develop the standard organized an internal working group, the purpose of which was to identify any relevant patents. With the help of lawyers and engineering consultants from over forty technology firms, the group identified and reviewed about 8,000 U.S. patent abstracts and about 800 patents, which had been assigned to over 100 patent owners.¹⁵⁹ This

155. Lerner & Tirole, *supra* 153, at 174 (“The standard setting effort began in July 1990, and the final MPEG-2 standard was approved in November 1994.”).

156. For more, see generally JAN VAN DER MEER, *FUNDAMENTALS AND EVOLUTION OF MPEG-2 SYSTEMS: PAVING THE MPEG ROAD* (2014) (discussing the development of MPEG-2).

157. Paul Backaus, *The Illusion of Motion*, PAULBAKAUS.COM (May 21, 2014), <https://paulbakaus.com/tutorials/performance/the-illusion-of-motion/> [https://perma.cc/A8RN-WACT].

158. This effect is commonly referred to as “the persistence of vision.” See generally Bill Nichols & Susan J. Ledermann, *Flicker and Motion in Film*, in *THE CINEMATIC APPARATUS* 96 (Teresa de Lauretis & Stephen Heath eds., 1980).

159. See HOVENKAMP, *supra* note 106, § 34.04[C] at 34–50 (“To determine which patents would be contributed to the pool, a number of firms participating in a ‘MPEG-2 Intellectual Property Working Group’ hired an expert and invited submissions of patents that might be relevant to MPEG-2 compliance. The expert reviewed some 800 patents assigned to approximately 100 parties, and ultimately concluded that several of the patents were ‘essential’ to compliance with the MPEG-2 standard—meaning that there were no technological alternatives to the claimed technologies. Of the patents identified as essential, most (27) were contributed to the pool.”).

work led to a consensus among the companies involved that they had found all (or nearly all) patents essential to MPEG-2.¹⁶⁰ At its launch, the MPEG-2 License included 25 patent families consisting of 102 essential patents. These covered many aspects of the standard, including spatial and temporal compression techniques, and methods of transmission.

After identifying these patents, the group developed a set of agreements that defined a new patent pool. A new limited liability company, “MPEG LA,” was formed to administer licensing.¹⁶¹ The group invited holders of all essential patents to join and made the pool open to any future members that wished to include standards-essential patents that they owned.¹⁶²

In April 1997, MPEG LA and the individual patent holders that had joined the MPEG-2 pool—Columbia, Fujitsu, General Instrument, Lucent, Matsushita, Mitsubishi, Philips, Scientific-Atlanta and Sony¹⁶³—submitted a letter to the Antitrust Division of the DOJ, requesting assurance that their planned pool did not violate the law or otherwise raise competition concerns. Two months later, on June 26, 1997, the DOJ responded favorably. Following a careful and lengthy analysis of the proposed pool, the letter concluded, “[i]t appears, however, that the proposed arrangement will not raise any significant competitive concerns.”¹⁶⁴ The MPEG-2 pool officially launched a short time later, on July 17, 1997.

Around this time, an outsider emerged. Although Lucent collaborated on the pool and joined in signing the letter sent to the DOJ, it elected to license independently.¹⁶⁵ Details of this decision are not well documented, but an interview subject directly involved in the pool offered a helpful account of when the news was relayed: “on the day of the announcement of the patent pool’s launch,” he explained, “Lucent told the other members of the group and MPEG LA that it planned not to join.”¹⁶⁶ According to this subject, one reason for Lucent’s reluctance to join was their successful internal licensing

160. See Letter from Garrard R. Beeney, Sullivan & Cromwell, to Joel I. Klein, Assistant Att’y Gen., U.S. Dep’t of Justice 11 (Apr. 28, 1997), <https://www.justice.gov/archive/atr/public/busreview/request-letters/302637.pdf> [<https://perma.cc/4J5V-AW5Y>] (“[T]he proposed licensing arrangement includes most, but not all, MPEG-2 essential patents.”); Letter from Joel I. Klein, Assistant Att’y Gen., U.S. Dep’t of Justice, to Garrard R. Beeney, Sullivan & Cromwell (June 26, 1997), www.justice.gov/archive/atr/public/busreview/215742.pdf [<https://perma.cc/3753-L3P5>] [hereinafter MPEG-2 Resonance Letter].

161. See *A History of Success—A Future in Innovation*, MPEG LA, <http://www.mpegla.com/main/Pages/AboutHistory.aspx> [<https://perma.cc/EA3M-XZ33>] (last visited Mar. 11, 2018).

162. *Id.*

163. See MPEG-2 Response Letter, *supra* note 160, at 2.

164. See MPEG-2 Response Letter, *supra* note 160, at 10.

165. See HOVENKAMP ET AL., *supra* note 106, at 34–49.

166. Telephone Interview with Horn & Geary, *supra* note 116.

capabilities. “Lucent was very well known for running a very strong and successful licensing program with their own portfolio which may have accounted for their decision,” this subject stated.¹⁶⁷ According to Josh Lerner and Jean Tirole, Lucent’s decision came down to compensation:

Lucent had a large internal licensing department with sufficient resources to conduct its own MPEG-2 licensing activities. Moreover, Lucent believed that two of its patents were most critical to the MPEG standard. Lucent felt that the licensing rate established by MPEG LA was lower than it could have been and decided not to join the pool. Lucent estimated that the higher royalty rates it would be able to charge by not joining the pool would more than offset the decreased fraction of the MPEG-2 market that would license its technology if it pursued its own licensing activities.¹⁶⁸

Like Lucent, Thomson also initially refused to join to the pool, preferring to independently license its patents.¹⁶⁹ As explained later in this case study and in the DVD case study that follows, however, it ultimately joined relatively early in the pool’s history, in July 2002.¹⁷⁰

The MPEG-2 pool’s royalty division formula treated all essential patents as equal in value—a view that may have not been shared by Lucent at the time.¹⁷¹ As an interview subject at MPEG LA explained, because any essential patent could block commercialization, all the patents arguably carried an equal value.¹⁷² “The patents included in this pool are all essential,” stated another subject, referring to debates about the issue among licensors.¹⁷³ “I don’t think anyone can say that one patent is *more* essential than another, because you need them all. They are all blocking.”¹⁷⁴ The subject went on to note, however, that “this was the first modern-day patent pool, and there were many who had reasons to be skeptical about its success.”¹⁷⁵

Lucent’s absence from the pool may have fostered some initial doubts in the market. As a subject at MPEG LA explained, “Lucent’s withdrawal added yet another element for them to be skeptical about.”¹⁷⁶ According to this

167. *Id.*

168. Lerner & Tirole, *supra* note 153, at 176.

169. Telephone Interview with Subject #3, *supra* note 124.

170. *Id.*

171. Telephone Interview with Subjects #12 and #13, *supra* note 147.

172. *Id.*

173. Telephone Interview with Horn & Geary, *supra* note 116.

174. *Id.*

175. *Id.*

176. *Id.*

subject, MPEG LA allayed these concerns with a straightforward explanation of the value they were offering:

We told [prospective licensees] that our program was voluntary and that Lucent had decided not to join. Despite this fact, we explained that the patents of the eight firms in the pool were essential, valuable, and worth paying for. We also explained that we were doing a lot of their homework for them because we were basically showing them the patent landscape they would otherwise have to research for themselves.¹⁷⁷

“People accepted the license we offered with the eight [patent holders],” explained a research subject at MPEG LA, adding, “the eight, by the way, grew rapidly to about ten in about six months.”¹⁷⁸ MPEG LA respected Lucent’s decision to go it alone but kept the door open for them to join anytime, “in the interest of including as much essential intellectual property as possible for the benefit of licensees,” a subject at MPEG LA explained, adding, “the extent to which the pool may have affected Lucent’s licensing efforts was not clear.”¹⁷⁹

Lucent was nevertheless steadfast in remaining an outsider. In March 2003, Alcatel, a French telecommunications company joined the MPEG-2 patent pool as a licensor.¹⁸⁰ In April 2006, Lucent and Alcatel agreed on a plan to merge their companies.¹⁸¹ Just two months later, with the merger underway, executives at Lucent realized that unless they acted fast, the company’s MPEG-2 patents would likely be included in the patent pool by virtue of Alcatel’s membership.¹⁸² (MPEG LA’s membership agreement required all members and their present or future “affiliates” to license essential patents to the pool.)¹⁸³ To prevent this, Lucent established a trust in Delaware, which it named the Multimedia Patent Trust (MPT).¹⁸⁴ Lucent was named as a beneficiary.¹⁸⁵ In November 2006, Lucent transferred its MPEG-2 essential patents to the trust.¹⁸⁶

177. *Id.*

178. *Id.*

179. Email from Horn & Geary, *supra* note 127.

180. Lucent Techs., Inc. v. Gateway, Inc., No. CIV. 02-2060-B(CAB), 2007 WL 2900484, at *1 (S.D. Cal. Oct. 1, 2007).

181. *See id.* at *1.

182. *See id.* at *2.

183. *See id.* at *4.

184. *See id.* at *2.

185. *See id.* at *6.

186. *Id.* The patents were U.S. Patent Nos. 4,958,226 and 4,383,272.

Alcatel-Lucent then sued several computer hardware manufacturers for infringing the patents held in the trust. The defendant in one suit was Microsoft.¹⁸⁷ There, Alcatel-Lucent filed a motion for summary judgment, holding that Microsoft's implementation of the MPEG-2 video standard in its Xbox video game console was infringing.¹⁸⁸ In response, Microsoft challenged the validity of the patents in the trust and argued for equitable estoppel based on Lucent's commitment to license the patents to MPEG LA.¹⁸⁹ Microsoft also argued in the alternative that even if the patents were valid, they were not essential to the MPEG-2 standard.¹⁹⁰ Microsoft argued, in other words, that the mere fact that its products abided by the MPEG-2 standard was not *prima facie* proof that it had infringed Lucent's patents.¹⁹¹ Finally, Microsoft asserted a series of counterclaims of patent infringement against Lucent.¹⁹² Ultimately, Alcatel-Lucent was unsuccessful on both fronts: the court held that the facts did not support a conclusion that Microsoft's products infringed Lucent's and did support Microsoft's patent infringement claims.¹⁹³

Matters grew worse for Alcatel-Lucent and MPT in 2007, when MPEG LA sued them for breach of contract in Delaware.¹⁹⁴ The complaint alleged that Alcatel-Lucent had promised to license *all* MPEG-2 patents that it could—an obligation that MPEG LA argued Lucent had failed to fulfill when it transferred the patents to MPT. The complaint stated, “the only purpose of the transfer was to avoid Alcatel's contractual commitment” in order “to extract additional royalties from MPEG-2 licensees.”¹⁹⁵

In late March, 2010, the suit settled—“literally in the middle of trial,” as one subject involved recounted.¹⁹⁶ As described in a court filing, the settlement

187. Lucent Techs., Inc. v. Microsoft Corp., 544 F. Supp. 2d 1080 (S.D. Cal. 2008).

188. *See id.* at 1087.

189. *See id.* at 1094, 1098.

190. *See id.* at 1102.

191. *See id.* at 1090–91.

192. *See id.* at 1096–1103.

193. Lucent Techs., Inc. v. Microsoft Corp., No. 06-CV-0684-H (CAB), 2008 WL 2872738, at *2 (S.D. Cal. July 23, 2008).

194. Press Release, MPEG LA, MPEG LA Sues Alcatel Lucent for Breach of MPEG-2 Patent Pool Contractual Obligations (Nov. 5, 2007), <http://www.mpegla.com/main/Pages/LegalAction.aspx> [<https://perma.cc/XD8N-P6P3>].

195. Amended Verified Complaint ¶¶ 6–7, MPEG LA, L.L.C., v. Lucent, No. 3317-VCL, (Del. Ch. Feb. 12, 2010), 2010 WL 519600; *see also* Scott M. Fulton III, *MPEG-2 Patent Holder, Licensing Agent in High-Def Codec Dispute*, BETANEWS (Nov. 6, 2007), <https://betanews.com/2007/11/06/mpeg-2-patent-holder-licensing-agent-in-high-def-codec-dispute/> [<https://perma.cc/JKD8-W9JV>].

196. Telephone Interview with Horn & Geary, *supra* note 116; *see also* Susan Beck, *We Surrender! After Two Days, Alcatel-Lucent Waves the White Flag in Patent Showdown*, AM. LAW. (Mar.

agreement required the MPT to subject the patents at issue in the Action pursuant to MPEG LA's usual procedures for determination of whether any of them were "MPEG-2 Essential Patents" or "MPEG-2 Systems Essential Patents."¹⁹⁷ MPT agreed that if the patents were determined to be essential, it would join the pool.¹⁹⁸

Thomson, as mentioned earlier, had initially elected to keep its patents outside of the MPEG-2 pool. They joined long before the episode involving Alcatel-Lucent's trust, however, in July 2002.¹⁹⁹ One research subject explained, "Technicolor [Thomson] was originally participating in discussions of the MPEG-2 Video patent pool, they stayed out and went as an independent. But later on, they experienced that they were not as successful as MPEG LA at sales, and they joined MPEG LA. So, they came back."²⁰⁰ Another subject directly involved with the decision explained that Thomson joined because it was impressed by MPEG LA's success in its early years.²⁰¹ Interestingly, Thomson's need to become a pool *licensee* may have also factored into their decision to join. "Thomson needed to become in its own right a licensee," added another subject.²⁰² "They made a lot of set-top boxes in that era, and they used MPEG-2. The good news is that Thomson became a licensee."²⁰³

As for Lucent, staying outside of the MPEG-2 pool appears to have been a costly strategy. According to multiple subjects interviewed, Lucent was unable to collect royalties that were appreciably higher than what they would have received as a member of the pool.²⁰⁴ This was because the pool provided a signal to licensees of what the value of the patents relating to the technology

26, 2010, 12:00 AM), [https://www.law.com/americanlawyer/almID/1202446807481/\[https://perma.cc/Z2WF-PVB3\]](https://www.law.com/americanlawyer/almID/1202446807481/[https://perma.cc/Z2WF-PVB3]).

197. Press Release, MPEG LA, MPEG LA Lawsuit Against Alcatel Lucent Settled (Mar. 29, 2010), <http://www.mpegla.com/main/Pages/LegalAction.aspx> [https://perma.cc/9C7Y-B3FF].

198. *Id.*; see also Exhibit A, Lucent Technologies, Multimedia Patent Trust v. Gateway, Inc., Trade Reg. Rep. P 75977 (C.C.H.) (S.D. Cal, October 1, 2007), 2007 WL 9431594.

199. Telephone Interview with Subject #3, *supra* note 124.

200. Telephone Interview with Subject #2 (July 15, 2017) (on file with author).

201. Telephone Interview with Subject #3, *supra* note 124.

202. Telephone Interview with Horn & Geary, *supra* note 116.

203. *Id.*

204. Telephone Interview with Subjects #12 and #13, *supra* note 147. Consistently, the court found no evidence that Alcatel-Lucent had demanded "supracompetitive" prices, arguing that this was just attorney speculation. Lucent Techs., Inc. v. Gateway, Inc., No. CIV. 02-2060-B(CAB), 2007 WL 2900484, at *17 (S.D. Cal. Oct. 1, 2007). This is consistent with the accounts laid out earlier, that Lucent was unable to use its outsider status to demand supracompetitive prices. *See id.*

was.²⁰⁵ Licensees apparently reasoned that, because any essential patent could block commercialization, all patents were approximately equal in value.²⁰⁶ Meanwhile, by suing licensees of the pool, Alcatel-Lucent exposed itself to counterclaims that led to findings of patent infringement on its part.²⁰⁷ The same court's finding that Lucent had not been infringed upon, meanwhile, raised fresh questions about the essentiality of some of Lucent's patents.²⁰⁸ Added to all of this was Lucent's opportunity cost. "In the period between 1997 when they decided to join and 2010 when this lawsuit forced them to join," explained an interview subject, "they left huge amounts of money on the table. Because you can't go back to get royalties that you missed when you should have been in the pool. Because that money goes out the door to licensors."²⁰⁹ In the end, all of Lucent's patents ended up in the pool.²¹⁰

D. OUTSIDE THE DVD PATENT POOLS (CASE STUDY)²¹¹

In the late 1980s, the ascendance of digital music CDs over cassette tapes set the stage commercially and technologically for Digital Versatile Disc (DVD) technology.²¹² Although analog systems that stored and played back movies from optical discs had existed since the late 1970s, none were widely adopted in the United States.²¹³ As a result, through the early 1990s, most Americans owned a VHS player—a device that played movies stored in analog

205. Telephone Interview with Horn & Geary, *supra* note 116.

206. This conclusion was drawn generally from discussions with interviewees.

207. Lucent Techs., Inc. v. Microsoft Corp., 544 F. Supp. 2d 1080, 1120 (S.D. Cal. 2008).

208. Steven Reynolds, *Setting the Record Straight on Upcoming Patent Rights Trial*, LUCENT-ALCATEL CEO BLOGS (Mar. 2010) ("That court decided that the MPT patents were not infringed by Microsoft's MPEG2 products. Obviously, and as is clarified by Bloomberg through its correction, Alcatel-Lucent can't be risking something that a court already determined that the MPT is not entitled to receive. The amount quoted is completely unrelated to the current trial.").

209. Telephone Interview with Horn & Geary, *supra* note 116.

210. *Id.*

211. This discussion pertains specifically to DVD Video and not recordable DVD media. For more information about recordable DVD standards, see Stephan Gauch, + vs -: *Dynamics and Effects of Competing Standards of Recordable DVD-Media*, in *THE DYNAMICS OF STANDARDS* 47 (Tineke M. Egyedi & Knut Blind eds., 2008).

212. See JIM TAYLOR, *DVD DEMYSTIFIED* 38 (2d ed. 2001) ("It was not until the development of compact disc digital audio in the 1980s that optical media again proved its worth in the world of bits and bytes, setting the stage for DVD.").

213. Julie Flaherty, *Bittersweet Times for Collectors of Laser Disc Movies*, N.Y. TIMES (Apr. 29, 1999), <https://nyti.ms/2v7Gk1e> [<https://perma.cc/K7YR-NU92>] (commenting on the success of DVD). One subject for this Article stated, "[l]aser discs with movies . . . did not have success on the market. Many companies thought before the launch of DVD that DVD would not take off. It has been a good surprise for everyone." See email from Alfred Chaouat, Senior Vice President of Licensing, Technicolor, to author (July 24, 2017).

form on cumbersome cartridges of magnetically charged tape.²¹⁴ When it was introduced in the late 1990s, DVD marked a leap ahead in quality and convenience, offering full-length movies in the then-new MPEG-2 format on elegant plastic discs the same size as CDs.²¹⁵ Although it was eventually usurped by high-definition Blu-Ray discs and streaming video, DVD was a commercial giant during its reign: by 2006, about eighty-one percent of American homes had a DVD player, a figure that surpassed that of VCR player ownership in that year.²¹⁶ The Microsoft Xbox and Sony PlayStation—two dominant videogame consoles of the 1990s and 2000s—also relied upon the DVD format for game data.²¹⁷ This success resulted from the work of two patent pools, one lone licensor, and many manufacturers who licensed from all three.

Warren Lieberfarb, former President of Warner Home Video, is widely credited for his instrumental role in encouraging the development of the DVD standard.²¹⁸ During his distinguished career working at leading film production companies—first as a financial analyst and later as a senior executive—Mr. Lieberfarb was, according to former colleagues, deeply intrigued by the idea of a digital video disc for decades.²¹⁹ He encouraged Toshiba to develop a prototype of the technology, which was demonstrated to electronics companies and industry stakeholders in 1994.²²⁰ Despite initial skepticism, the

214. See generally TAYLOR, *supra* note 212, at 19, 24–37 (discussing the history of VHS and other video technology and reporting that 87% of all U.S. households owning at least one VCR as of the book’s publication date, which was 1998).

215. See *id.* at 60–70 (discussing the introduction of DVD players in the United States).

216. See, e.g., *DVD Players Overtake VCRs*, CNN MONEY (Dec. 26, 2006, 9:34 AM), http://money.cnn.com/2006/12/26/technology/dvd_vcr [<https://perma.cc/VT9L-EJEP>].

217. See, e.g., Steve Traiman, *It’s All in the Games*, BILLBOARD MAG., Mar. 31, 2001, at 62, 69 (noting that Nintendo’s Gamecube console relied on a variant of DVD that used discs with smaller diameters).

218. See, e.g., Martin Dale, *Warren Lieberfarb: The History of DVD and Cable Networks Highlights the Tremendous Value of Classic Films*, VARIETY (Oct. 12, 2014, 11:08 AM) (“Warren Lieberfarb is universally recognised as the ‘architect of the DVD’ . . .”), <http://variety.com/2014/film/global/warren-lieberfarb-the-history-of-dvd-and-cable-networks-highlights-the-tremendous-value-of-classic-films-1201328060/> [<https://perma.cc/6RN8-Z7MH>]; James Greenberg, *Private Sector; The Would-Be King of DVD*, N.Y. TIMES (Nov. 24, 2002), <http://www.nytimes.com/2002/11/24/business/private-sector-the-would-be-king-of-the-dvd.html> [<https://perma.cc/9KWV-F7AW>] (reporting that many in the film industry credit Lieberfarb “with dreaming, cajoling and bullying the DVD into existence”). Similarly, a research subject for this study emphasized Lieberfarb’s importance in bringing about the DVD. See email from Alfred Chaouat to author, *supra* note 213.

219. See Greenberg, *supra* note 218 (quoting the former executive of AOL Time Warner as saying that Mr. Lieberfarb’s focus on the DVD was “the most consuming manifestation I’ve ever seen in an individual”).

220. *Id.*

film and technology industries came to support the development of a new standard, thanks in large part to Mr. Lieberfarb's lobbying.²²¹ After further research and experimentation, two teams composed of leading technology firms emerged with the most promising solutions: Philips and Sony co-developed a format it called "Multimedia CD" or "MMCD";²²² Toshiba, meanwhile, asked Hitachi, Matsushita (Panasonic), Mitsubishi, Victor (JVC), Pioneer, and Thomson to help it further develop its 1994 prototype.²²³ This work led to a format the group called the "Super Disc" or "SD."²²⁴ Anxious about the possibility of a wasteful format war like the one that slowed the adoption of VHS over a decade earlier, Apple, Microsoft, Sun Microsystems, Dell, and other manufacturers, urged these two teams to combine.²²⁵

Cooperation came in 1995, but it would be short-lived. Sony and Philips agreed to join the "SD" group to work on a single format that would incorporate elements of both the MMCD and the SD formats.²²⁶ The collaborators agreed to call the new format the DVD.²²⁷ Notably, this development work was not mediated by a standard-setting organization, but instead, was largely a private venture that operated under the auspices of "The DVD Consortium" (later renamed "The DVD Forum").²²⁸ As a result, details of the DVD standard were kept confidential and available only to licensees who signed a nondisclosure agreement.²²⁹ Two subjects directly involved

221. See TAYLOR, *supra* note 212, at 37–39 (noting that optical discs rely on a method of storing information through the use of divots to represent bits, a principle understood since Charles Babbage's seminal work in developing digital programmable computers).

222. See *id.* at 40–60; Letter from Garrard R. Beeney, Sullivan & Cromwell, to Joel I. Klein, Assistant Att'y Gen., U.S. Dep't of Justice (July 29, 1998), <https://www.justice.gov/atr/page/file/1020341/download> [<https://perma.cc/8SGD-ZDVW>] [hereinafter DVD3C Request Letter].

223. Email from Alfred Chaouat to author, *supra* note 213.

224. Letter from Carey R. Ramos et al., Paul, Weiss, Rifkind, Wharton & Garrison to Joel I. Klein, Assistant Att'y Gen., Antitrust Div. of the U.S. Dep't of Justice 6 (Oct. 9, 1998), <https://www.justice.gov/sites/default/files/atr/legacy/2014/01/08/302365.pdf> [<https://perma.cc/269A-WBFT>] [hereinafter DVD6C Request Letter]; see also *Electronic Giants Battle On*, NEXT GENERATION, Nov. 1995, at 19 (discussing the battle between MMCD and the SD formats).

225. See TAYLOR, *supra* note 212, at 48–49 (discussing reconciliation between the two camps).

226. See *id.*

227. See *id.* at 50.

228. *Id.*; Telephone Interview with Alfred Chaouat, Senior Vice President of Licensing, Technicolor (July 19, 2017) (explaining the change in name).

229. Discussing the DVD standard, one research subject emphasized the difference between "technical essentiality" and "commercial essentiality." The former, the subject explained, relates to patents that are necessarily infringed by any device that follows a standard; the latter, by contrast, describes patents that are infringed by devices that follow the standard

independently confirmed that participants in the DVD Forum were subject to a FRAND obligation, however.²³⁰ The group finalized the first DVD specification in late 1995.²³¹

The collaborators wished to pool their patents under a single license, but they were unable to come to an agreement. At a June 1996 DVD conference, speakers announced that the ten companies had agreed to form a patent pool in order to streamline licensing.²³² “The goal was to form one pool,” stated one subject directly involved.²³³ On August 2, 1996, Sony and Philips announced that they would begin licensing their patents jointly and invited the other eight companies to join in.²³⁴ Pioneer later joined Sony and Philips, and the three companies formed a pool called the “DVD3C Licensing Group.”²³⁵ Six of the remaining companies formed a pool they called the “DVD6C Licensing Group.”²³⁶ Thomson, meanwhile, decided to license independently.²³⁷

A research subject directly involved with the attempt to form a single pool commented, “ultimately, the goal of a single pool failed because various groups had different views as to how to share the royalties.”²³⁸ This subject went on to explain that “the fundamental difference was whether the royalties should be divided on a per-patent basis only or should also take into account the total contribution of a party to the optical technology concerned.”²³⁹ Another subject with knowledge of the episode commented, “frankly, they couldn’t agree on royalties. That was the problem. They were never able to get there.”²⁴⁰ Yet another individual involved explained:

The discussions for formation of a potential pool including all DVD Forum companies took many months, did not reach a consensus and finally led to the formation of two separate pools . . . in great part

in a manner that makes the device commercially desirable or cost effective. Telephone Interview with Horn & Geary, *supra* note 116 (“There’s a lot of mechanical stuff in a DVD player. So, let’s say the standard recites that you have to be able to jump across ten tracks within a certain number of milliseconds but it doesn’t specify how you could do that. There may be many ways you could actuate the system to make that jump, some of which are preferable to the manufacturer. Those practices may be commercially essential.”).

230. Telephone Interview with Subject #2, *supra* note 200; email from Alfred Chaouat to author, *supra* note 213.

231. See TAYLOR, *supra* note 212, at 51.

232. See *id.* at 54.

233. Telephone Interview with Subject #2, *supra* note 200.

234. See TAYLOR, *supra* note 212, at 56.

235. See generally DVD3C Request Letter, *supra* note 222 (describing the pool).

236. DVD6C Request Letter, *supra* note 224 (describing the pool).

237. Telephone Interview with Subject #3, *supra* note 124.

238. Telephone Interview with Subject #2, *supra* note 200.

239. *Id.*

240. Telephone Interview with Horn & Geary, *supra* note 116.

because Philips would not accept to decrease its share in the intended pool. Thomson decided that it was better off financially, and as a respected licensor, to continue to license its patents separately, in a single license incorporating all technologies used in the DVD player.²⁴¹

For its part, Thomson appears to have had a few reasons for remaining independent. A research subject explained that in part, the company viewed certain patents it held as having special value:

All essential patents in a patent pool have, in general, the same value. At that time, Thomson still owned some fundamental patents addressing the way the pits are read by an optical laser beam, which, from our perspective, was much more valuable than the DVD essential patents dealing with the multi-angle view, for example. So, we decided not to join any of the DVD patent pools.²⁴²

In addition to this, however, Thomson felt the most comfortable working with its own licensing staff purely because very few other companies involved in the pools had a long track record for this kind of work. The research subject continued:

Another reason why Thomson did not join the 6C patent pool is the uncertainty about who would be the agent. We knew that Philips had great experience and talent through their joint CD licensing program with Sony. We were not so sure if the other 6C pool members had the ability to manage a patent pool well, however. Also, we were already managing our own successful CD player licensing program. The decision to join a pool has to do with the rate and your share of it, but also how you assess the capabilities of the licensing agents. Licensing agents are not all equal.²⁴³

As a result, manufacturers of DVD players would need to obtain essential patent licenses from both pools and Thomson.

Despite the fragmentation, the three licensors requested royalties that resulted in roughly comparable royalty rates relative to the number of patent-families or inventions licensed. In a letter requesting review and approval from the DOJ, for instance, the 3C licensing group (Philips, Sony, and Pioneer)

241. Email from Subject #5 to author, *supra* note 122.

242. Email from Alfred Chaouat to author, *supra* note 213. This subject went on to note that Thomson spearheaded an important Blu-Ray patent licensing pool, however, and emphasized that the decision to join or pool or remain independent is done “one a case-by-case basis.”

243. Telephone Interview with Alfred Chaouat, *supra* note 228.

stated that their pool would contain 115 DVD player patents.²⁴⁴ Based on discussions with a subject involved and a review of essentiality lists, this figure refers to patent families, each of which may have included individual patents granted in different countries and some divisionals as well.²⁴⁵ The 3C pool stated that it would charge DVD player manufacturers 3.5% of net sales with a minimum of \$7 per unit sold, which would drop to \$5 per unit sold beginning in the year 2000.²⁴⁶ Because most DVD players sold for under \$200, the minimum dollar rates were the most important after several years.²⁴⁷ Before the year 2000, the 3C pool collected a per-patent-family rate of about \$0.06.²⁴⁸ From the year 2000 onward, the pool yielded a per-patent-family rate of about \$0.043 for each player.²⁴⁹ The DOJ replied favorably on December 16, 1998, stating that the 3C pool raised no antitrust concerns.²⁵⁰ With these assurances, the DVD3C pool began offering licenses soon after.

The 6C group (Hitachi, Matsushita, Time Warner, Toshiba, and others) submitted a request for business review to the DOJ at around the same time, on October 9, 1998.²⁵¹ They would license forty-four DVD player patents at a rate of 4% of net sales per player, with a minimum of \$4 per player.²⁵² This figure refers to patent families, each of which may have included individual patents granted in different countries and divisionals as well.²⁵³ Again, because DVD player prices were generally low enough, it is safe to assume that the

244. See DVD Business Review Letter, *supra* note 100, at 4 (“[T]here are 115 patents in all for the manufacture of DVD players, and 95 for the manufacture of the discs themselves.”).

245. Email from Alfred Chaouat to author, *supra* note 213; see also *Licensing: DVD-Video/ROM Disc (Joint)*, PHILLIPS, <http://www.ip.philips.com/licensing/program/29/dvd-video-rom-disc-joint> [<https://perma.cc/6TXR-8UQ4>] (last visited Mar. 11, 2018) (offering a list of patents granted in different countries).

246. See DVD3C Request Letter, *supra* note 222.

247. Telephone Interview with Ruud Peters, *supra* note 118. For a more detailed view of these numbers, see the tables and accompanying discussion *infra* Section IV.B.

248. *Id.*

249. *Id.*

250. Interestingly, the DOJ addressed the outsider concern in its response, although not with respect to the two DVD pools or Thomson. Instead, it discussed the possibility that a member of the DVD3C pool might refuse, at some future time, to license essential patents it might acquire—outsiderism by an insider, as it were. The DOJ did not believe this would seriously dampen the efficiencies of the pool. See DVD Business Review Letter, *supra* note 100, at 14 n.58 (“Transaction costs to licensees would almost certainly be somewhat lower if these later patents were included in the pool, instead of being subject to separate negotiations. However, the fact that this pool might not enable the realization of all potential efficiencies of pooling patents in this area does not mean that the efficiencies that it does create are insubstantial or that the arrangement is anticompetitive or unlawful.”).

251. See DVD6C Request Letter, *supra* note 224.

252. *Id.* at Exhibit 2 (on file with the author) (listing the forty-four patents).

253. *Id.* at 13.

minimum price per player was the most relevant. Based on this, the DVD6C group collected per-patent-family rates of approximately \$0.09 for players. The DOJ responded favorably on June 10, 1999.²⁵⁴ “By reducing what would otherwise be six licensing transactions to one,” the DOJ wrote, “the pool would reduce transactions costs for Licensors and licensees alike. By ensuring that each Licensor’s patents will not be blocked by those of the other five, the pool would enhance the value of all six Licensors’ patents.”²⁵⁵ In the DOJ’s view, it seemed that some cooperation was better than none.

This leads to Thomson. According to a subject directly involved, prior to July 2002, Thomson licensed both its MPEG-2 and DVD patents independently.²⁵⁶ At that time, the rate it charged DVD player manufacturers for both sets of patents was \$1.7 for each DVD player sold.²⁵⁷ In July 2002, Thomson decided to join the MPEG-2 patent pool, as discussed earlier,²⁵⁸ and it lowered the rate of its DVD patents to 1.3% of the net selling price of each player, with a minimum of \$1.3 per unit.²⁵⁹ Thomson’s portfolio included 10 essential patent families.²⁶⁰ As with the two pools, each patent family included numerous patents filed in different countries as well as divisionals.²⁶¹ At a rate of \$1.3 per sale, this equated to a per-patent-family rate of \$0.13.

Although this effective per-patent-family rate is higher than that of the 3C and 6C pools, a research subject explained that some licensees who held patents Thomson wished to license paid Thomson lower rates. “We concluded some bilateral licenses (i.e., including a license back for Thomson) at a lower rate than the standard rate when the licensee owned relevant DVD patents that we were using in our products. Otherwise, we succeeded to license our patents at the standard rate.”²⁶² This comment connected with an opinion shared by another research subject, who stated,

254. See Letter from Joel I. Klein, Assistant Att’y Gen., U.S. Dep’t of Justice, to Carey R. Ramos, Paul, Weiss, Rifkind, Wharton & Garrison (June 10, 1999), <https://www.justice.gov/sites/default/files/atr/legacy/2012/08/01/2485.pdf>. [<https://perma.cc/23X3-S793>] [hereinafter DVD6C Response Letter] (responding favorably to the proposed pool).

255. *Id.*

256. Telephone Interview with Research Subject #3, *supra* note 228.

257. *Id.*

258. Press Release, Thomson Multimedia, Thomson Joins MPEG LA Patent Pool (July 11, 2002), www.sec.gov/Archives/edgar/vpr/0204/02048954.pdf [<https://perma.cc/WNS2-EMC3>].

259. Telephone Interview with Alfred Chaouat, *supra* note 228.

260. *Id.*

261. *Id.*

262. Email from Alfred Chaouat to author, *supra* note 213.

You need to understand that this is the asking price. In bilateral negotiations there's always a difference between the asking price and the price you finally settle on—a negotiation margin. When you have a pool, by contrast, you always have a fixed rate.²⁶³

The per-patent-family rates for players collected by all three licensors were not vastly different in part because there was a mutual awareness that the aggregate cost for licensees could not be too high. Simply put, the licensors set their royalties in light of one another. The DVD6C pool signaled this when it wrote to the DOJ, “[t]he royalty rates proposed by the DVD pool are reasonable, especially when compared to the rates proposed by the MPEG-2 pool for patents used in DVD products or when compared to the rates proposed by the Sony/Philips/Pioneer 3-party DVD pool.”²⁶⁴ When asked if this showed that the 6C group looked to the 3C group for a baseline, a research subject directly involved commented, “I think that is a reasonable conclusion.”²⁶⁵ A licensing expert directly involved with licensing at Thomson also explained, “Thomson’s rate was set based on the rates set up by the two DVD patent pools.”²⁶⁶ In short, there was signaling among the two pools and Thomson.

A 2004 dispute in the District of Delaware involving the 6C pool illustrates the willingness of licensees to push back against independent rates they perceive as unreasonable in light of pool rates. *Matsushita Electrical Industrial Co. v. Cinram International, Inc.* involved a company that sought to license certain DVD disc patents directly from the individual members of the 6C pool.²⁶⁷ The pooling agreement allowed the companies to do this. The licensee was upset, however, because the per-patent-family rate requested by each licensor outsider of the pool was higher than the per-patent-family rate that the pool offered.

Cinram maintains that the structure of the 6C Pool discourages individual licenses because such licenses would undercut the pool price. . . . Cinram explains that the cost for individual licenses from four of the six 6C Pool members totaled \$0.11. Cinram points out that this total substantially exceeds the \$0.05 per disc royalty that it

263. Telephone Interview with Subject #2, *supra* note 200.

264. DVD6C Request Letter, *supra* note 224, at 20.

265. Telephone Interview with Subject #2, *supra* note 200.

266. Email from Alfred Chaouat to author, *supra* note 213.

267. *See Matsushita Elec. Indus. Co. v. Cinram Int'l, Inc.*, 299 F. Supp. 2d 370 (D. Del. 2004).

currently pays for a 6C Pool License, thereby making individual licenses entirely impractical.²⁶⁸

Interestingly, the District of Delaware rejected this argument based on its finding that the rates charged by the pool fell well below the “objective value” of the patents.²⁶⁹

The DVD licensing story fails to support the theory that outsiders will ask for royalties so excessive that licensees will be unable to bear the aggregate cost. Rather, in line with the MPEG-2 story, this episode seems to show that the pricing information published by patent pools (i.e., royalty rate announcements) sets a baseline for negotiations that take place outside of the pool and even rates charged by complementary pools. As explored in Part IV, this spillover benefit may be viewed as an unappreciated benefit of patent pools.

IV. ASSESSING THE IMPACT OF OUTSIDERS

The foregoing study shows that the royalty rates set by patent pools tend to limit the royalty rates that outsiders ask for and receive. This finding directly conflicts with the theory that outsiders will tend to undermine the benefits of patent pools. This is not to say, however, that the rate charged by outsiders and secondary pools is not relatively higher than the rate collected by individual members in a pool. In the DVD episode, for instance, some licensors collected relatively more than others. Should the higher relative rates in such settings be viewed as an “outsider premium?” To aid regulators, this Part introduces a technique for estimating the cost that a licensee either incurs or saves in the presence of an outsider. This technique is then applied to real-world financial and industry data collected in the foregoing study. The results indicate that, surprisingly, licensees may pay less in settings where cooperation among

268. *Id.* at 378.

269. *Id.* at 379 (“The Second Circuit has stated that the only valid test to prove that an alternative is too costly to be a realistic alternative is whether the price for such a license, in an objective sense, is higher than the value of the intellectual property rights being conveyed. In accord with this reasoning, the court concludes that the per disc royalty differential only causes the individual licensing option to be an unrealistic alternative if it is higher than the value of the DVD rights conveyed. The court finds that the facts at bar do not show this to be the case.”) (internal citations omitted); *Buffalo Broad. Co. v. Am. Soc. of Composers, Authors & Publishers*, 744 F.2d 917, 927 (2d Cir. 1984) (“Even if the blanket license is objectively the ‘better buy’ for most users, the program license would be a realistic alternative so long as it was fairly priced for those who might find it preferable for reasons other than price. But if the program license were available only at a price beyond any objectively reasonable range, the ‘bargain’ nature of the blanket license would not immunize it from characterization as a restraint.”).

licensors is slightly fragmented than they would pay in a setting where outsiders were induced to join a single pool.

A. A METHOD FOR ESTIMATING OUTSIDER COSTS AND BENEFITS

Do licensees pay more when outsiders are present than they would pay to a unified pool? This question asks one to compare reality as it is to a hypothetical world where no outsiders or secondary pools exist—i.e., a grand coalition where all relevant patent holders are joined. Evidence presented in the foregoing case studies indicates this is an unrealistic ideal, of course. Some outsiders simply prefer to go it alone, sometimes for idiosyncratic reasons. Unrealistic as it may be, however, a grand coalition hypothetical allows for a head-on quantitative assessment of the outsider concern. The following discussion presents a method of comparing the costs that a licensee incurs in settings with and without outsiders.

The greatest challenge in developing a picture of a grand coalition is determining what total royalty rate such a patent pool would charge licensees. Research subjects confirmed that the royalty rate set by a patent pool strikes a balance between what it takes to retain licensors and to offer reasonable terms to licensees over the course of a license.²⁷⁰ Recall from Part II of this Article that the amount licensors receive in most modern pools is determined by a formula, rather than through individual deals with each licensor who joins.²⁷¹ Earlier scholarship has shown that nearly all patent pools, historical and contemporary, have adopted this “rough and ready” approach to royalty divisions.²⁷² The two most common methods pools use to apportion royalties are “per-capita” and “per-patent.”²⁷³ Many patent pools use combinations of these two approaches as well.²⁷⁴ As a research subject for this Article explained, some pools will divide, say, twenty percent of their incoming royalties equally among the patent owners and the remaining eighty percent may be divided based upon the number of patents each member has licensed.²⁷⁵ A subject explained that a problem with a simple “per-patent” approach is that it encourages members of the pool to file many “divisional” patent applications relating to just one invention because doing so increases the raw number of patents upon which members’ royalties are based.²⁷⁶ To remedy this issue,

270. Email from Subject #11 (July 27, 2017) (on file with author).

271. Mattioli, *supra* note 12, at 439–55.

272. *See id.* at 462.

273. *See id.* at 446–47.

274. *Id.*

275. Telephone Interview with Subject #8 (July 15, 2017) (on file with author); email from Alfred Chaouat to author, *supra* note 213.

276. *Id.*

subjects explained, some recent pools have limited the number of patents that may be included in per-patent calculations, either by limiting the number of divisionals to be counted, or basing the division not on the raw number of patents but instead on the number of patent families contributed by a licensor.²⁷⁷ In light of these observations, a foundational assumption in this exercise is that a patent pool that includes all relevant patents will include a royalty-division formula of some kind.

This leads to a second assumption: in order to entice all outsiders to join as members, a grand coalition would need to deliver to all outsiders royalties that are at least as great as those they can already collect outside of the pool. One could argue quite fairly that perhaps a slightly lower rate than this would be enough to entice some outsiders to join, in light of the transaction cost savings that patent holders enjoy by belonging to pools. On the other hand, this study has revealed that most outsiders enjoy the efficiencies of robust internal licensing departments. For this reason, it is difficult to guess whether an outsider would be willing to give up some of its royalty returns in exchange for the efficiencies of belonging to a pool, and if so, how much. For these reasons, this exercise proceeds on the assumption that, to induce all licensors to join, a single pool must deliver to the highest-paid outsider royalties at least as great as those that outsider could draw on its own.

As a threshold matter, then, it is necessary to determine who the highest-paid licensor is and how much that licensor collects for each product that its licensees sell. In the course of conducting the studies in this Article, I received directly from research subjects and documentary sources a wealth of industry pricing data as well as the royalty rates charged by patent pools and individual licensors. In the practical example that follows, data from the DVD licensing industry are presented.

To aid in this analysis, it is helpful to represent the foregoing assumptions as equations. Equation 1, below, shows the total per-licensee royalty rate that a patent pool using a per-capita royalty division formula would need to charge in order to bring in an outsider that collects a per-licensee rate of “*RateOutsider*.” Here, n represents the total number of patent holders in the pool.

Equation 1: Royalty Rate Charged by Unified Pool Using Per-Capita Formula

$$Rate_{PC} = Rate_{Outsider} \times (n + 1)$$

277. *Id.*

This equation assumes that a patent pool is driven strictly by a royalty division formula and that it has not made a special agreement that has resulted in compensating the outsider more, comparatively, than the other members. This assumption might be challenged, but it seems reasonable, as existing members of a pool would likely disfavor disproportionately benefiting a reluctant member. For comparison, Equation 2, below, shows the total per-licensee royalty rate (“*RatePP*”) under a per-patent approach. Here, “*NumInside*” is the number of patents in the pool before the outsider joins, “*RateOutsider*” is the royalty rate the highest-paid outsider draws, and “*NumOutside*” is the number of relevant patents owned by that outsider.

Equation 2: Royalty Rate Charged by Unified Pool Using Per-Patent Formula

$$RatePP = (RateOutsider/PatentsOutsider) \times (NumInside + NumOutside)$$

To calculate the royalty rate that would be charged by a unified pool that uses a combination of the per-capita and per-patent approach, one can multiply the “*RatePP*” and “*RatePC*” values by their relative weights (e.g., 20% and 80%) and take the sum. The sum is referred to below as “*RateHypo*.”

Next, one can compare these hypothetical rates to the royalty rate that licensees pay all licensors in reality. This latter amount, represented by “*RateActual*” below, can be derived by adding the individual rates charged by each pool and each licensor. The difference between these values is a licensee’s total royalty cost or savings by working with a single pool as opposed to working with a pool and one or more outsiders.

Equation 3: Calculation of Rate Increase Due to Outsider Inclusion in Pool

$$RatePremium = RateHypo - RateActual$$

It is also necessary to consider transaction costs. For a licensee, working with a single pool involves just one transaction, compared to the multiple transactions necessary to work with, say, two pools and an outsider. The transaction costs conserved (“*TCostsSaved*”) by working with a unified pool, or grand coalition (“*TCostsGC*”), instead of a partial coalition involving multiple pools and outsiders (“*TCostsPC*”) can be represented as follows:

Equation 4: Transaction costs conserved under unified pool (per-licensee)

$$TCostsSaved = TCostsPC - TCostsGC$$

Bringing this all together, one can determine the total increase or decrease in cost to each licensee (“*OutsiderPremium*” below) by subtracting the transaction costs conserved by the rate increase incurred:

Equation 5: Calculation of Outsider Premium

$$\textit{OutsiderPremium} = \textit{RatePremium} - \textit{TCostsSaved}$$

If “*OutsiderPremium*” is positive, then licensees are better off under current conditions (licensing from the pool and outsider) than they would be if the outsider were induced to join the pool; if “*OutsiderPremium*” is negative, then licensees should wish for the pool to raise its rates to induce the outsider or outsiders to join.

Ultimately, the analysis boils down to comparing two numbers: the costs licensees incur in reality against those they would incur in a setting with a single pool that has raised its rates to pull in outsiders.

B. ESTIMATING THE IMPACT OF OUTSIDERS ON DVD LICENSEES

This discussion applies real-world financial and patent data gathered from the study in Part III to the method described in the preceding discussion. The result is a rough estimate of the impact, in cost, of outsiders on DVD licensees. The results are surprising: arguably, licensees fare *better* in the slightly fragmented licensing landscape that exists than they would in a setting with a single pool. The implications of this conclusion are explored further toward the end of this Article.

Drawing upon the study in Part III, the table below lists the number of patent families and royalty rates charged by DVD patent holders. Although research subjects indicated that outsiders such as Thomson sometimes agreed to accept rates lower than the rates they asked for, this study will rely on the “asking price” because this was reportedly the typical amount Thomson collected.

Table 1: DVD Video Licensing Rates (Per Unit Sold)

LICENSOR	PATENT FAMILIES	ROYALTY RATES	ROYALTY RATES (DOLLARS PER-PATENT-FAMILY)
DVD3C (3 LICENSORS)	115	\$7 before yr. 2000 \$5 after yr. 2000 (alt: 3.5% NSP ²⁷⁸)	\$0.06 (later \$0.043)
DVD6C (6 LICENSOR)	44	minimum: \$4 (alt: 4% NSP)	\$0.09
THOMSON / TECHNICOLOR (1 LICENSOR)	10	\$1.3 (alt: 1.3% NSP)	\$0.13

In addition to the minimum per-patent-family royalty rates that appear in Table 1, it is helpful to determine the actual per-patent-family royalty rates for years in which the minimum did not apply. As Table 1 shows, all licensors based their royalty rates on a percentage of the net selling price (NSP) of a DVD player until that percentage fell below a certain number—\$100 in the cases of DVD6C and Thomson. Drawing upon sales data published by the Consumer Electronics Association, Table 2 reflects the patent royalties a licensor would have collected from each licensor for an average-priced DVD player in the years 1997–2004.²⁷⁹ This range of years was selected because it coincided with the introduction and growth of DVD.

278. NSP signifies “Net Selling Price.” This is shown as an alternate measure of royalties owed. If the percentage shown in the table multiplied by a product’s NSP exceeds the minimum, the higher number was owed. Looking to the first row for example, if a DVD player was sold in the year 2001 for \$250, then 3.5% of this would have equaled \$8.75. Licensees would have owed this sum because it is higher than the minimum of \$5 listed for that time.

279. See *Cost of DVD Players*, DATA360, http://www.data360.org/dsg.aspx?Data_Set_Group_Id=497 [<https://perma.cc/65T8-87PX>] (last updated Sept. 7, 2006).

Table 2: DVD Video Licensing Costs (1997–2004)
(asterisks indicate that the minimum licensing rate has been reached)

YEAR	AVG. PRICE OF DVD PLAYER	DVD6C ROYALTIES PER UNIT SOLD	DVD3C ROYALTIES PER UNIT SOLD	THOMSON ROYALTIES PER UNIT SOLD	TOTAL LICENSING COSTS PER UNIT SOLD
1997	\$489.97	\$19.60	\$17.15	\$6.37	\$43.12
1998	\$390.18	\$15.61	\$13.66	\$5.07	\$34.34
1999	\$270.00	\$10.80	\$9.45	\$3.51	\$23.76
2000	\$201.55	\$8.06	\$7.05	\$2.62	\$17.74
2001	\$165.00	\$6.60	\$5.78	\$2.15	\$14.52
2002	\$142.00	\$5.68	\$5.00*	\$1.85	\$12.53
2003	\$123.00	\$4.92	\$5.00*	\$1.60	\$11.52
2004	\$108.60	\$4.34	\$5.00*	\$1.41	\$10.76

These amounts may now be compared to the hypothetical royalties that a single pool would charge licensees.

How much would a single pool need to charge to entice the highest-paid outsider to join? First, one must determine which entity is the highest-paid licensor. Thomson's profits for each product sold appear in Table 2. It is possible that a member of the DVD3C or DVD6C pool earned more than Thomson for each product sold. It is difficult to know this, however, because the formulas that apportion royalties among the three members of the DVD3C pool and the six members of the DVD6C pool are confidential.²⁸⁰ If the pools relied upon simple per-capita divisions, however, then Thomson always collected more than any member of the 3C or 6C pool for each net sale. If the formulas were more complex (which the business review letters indicate), then it is possible that one member of the 3C group could have collected more than Thomson at any time.²⁸¹ In the interest of keeping the final estimates conservative, however, one may select Thomson's royalties as a

280. See DVD Business Review Letter, *supra* note 100, at 6 ("The allocation of royalties among the Licensors is not a function of the number of patents contributed to the pool.").

281. See *id.*

measure of the highest amount any member would need to collect in a unified pool.²⁸²

Now it is useful to consider what total rate a patent pool using the various royalty-division rules outlined in the prior discussion would need to charge to ensure that Thomson received at least the level of royalties that it was able to collect independently. First, we can consider a formula based upon the number of patents infringed by a product, defined earlier in Equation 2. As explained earlier in this Article, the *per-patent-family* rate charged by a pool is a more accurate indicator of the value each member brings to the table than a *per-patent* rate and is reflective of the formulas that pools use in practice. For that reason, this example considers a formula that apportions royalties based on the number of patent families contributed. Thomson, as reported in Table 1, would have ten patent families to contribute to the pool. Therefore, the *per-patent-family* rate charged by the pool can be calculated simply by dividing Thomson's return (in Table 2) by ten. A flaw in this approach, of course, is the fact that patent composition may have changed during the period (1997–2004). As explained earlier, patents may have been added to or removed from pools. As a result, the calculation in Table 3 is approximate.

282. This assumption does not hold in all cases, as the 3C or 6C pools reach their royalty minima. However, the limitation of this assumption does not undermine the conclusion that pools consolidate at the highest royalty rate.

Table 3: Hypothetical Royalties Per Product Sold (Pro-Rata Formula)

YEAR	PER-PATENT-FAMILY RATE	DVD6C ROYALTIES (PER UNIT SOLD)	DVD3C ROYALTIES (PER UNIT SOLD)	THOMSON ROYALTIES (PER UNIT SOLD)	TOTAL LICENSING COSTS (PER UNIT SOLD) ("RATEPP")
1997	\$0.64	\$28.03	\$73.26	\$6.37	\$107.65
1998	\$0.51	\$22.31	\$58.31	\$5.07	\$85.68
1999	\$0.35	\$15.44	\$40.37	\$3.51	\$59.32
2000	\$0.26	\$11.53	\$30.13	\$2.62	\$44.28
2001	\$0.22	\$9.46	\$24.73	\$2.15	\$36.34
2002	\$0.19	\$8.14	\$21.28	\$1.85	\$31.27
2003	\$0.16	\$7.04	\$18.40	\$1.60	\$27.04
2004	\$0.14	\$6.20	\$16.22	\$1.41	\$23.83

What would the unified pool need to charge if it relied upon a per-capita formula? Referring to Equation 1, the information in Table 1, and the assumption that Thomson is the highest-paid licensor, the amounts under this hypothetical can be calculated, as shown in Table 4. To clarify, the DVD3C column receives three-times Thomson's rate, and the DVD6C pool receives six-times. Total licensing costs to a licensee appear in the right-most column.

Table 4: Hypothetical Royalties Per Product Sold (Per-Capita Formula)

YEAR	DVD6C ROYALTIES (PER UNIT SOLD)	DVD3C ROYALTIES (PER UNIT SOLD)	THOMSON ROYALTIES (PER UNIT SOLD)	TOTAL LICENSING COSTS (PER UNIT SOLD) ("RATEPC")
1997	\$38.22	\$19.11	\$6.37	\$63.70
1998	\$30.42	\$15.21	\$5.07	\$50.70
1999	\$21.06	\$10.53	\$3.51	\$35.10
2000	\$15.72	\$7.86	\$2.62	\$26.20
2001	\$12.90	\$6.45	\$2.15	\$21.50
2002	\$11.10	\$5.55	\$1.85	\$18.50
2003	\$9.60	\$4.80	\$1.60	\$16.00
2004	\$8.46	\$4.23	\$1.41	\$14.10

A comparison of the rates appears below:

Table 5: Actual Versus Hypothetical Royalty Cost to Licensees Per Unit Sold

YEAR	RATEACTUAL: ACTUAL COST TO LICENSEES	RATEPC: HYPOTHETICAL RATE TO LICENSEES UNDER PER-CAPITA ALLOCATION	RATEPP: HYPOTHETICAL RATE TO LICENSEES UNDER PRO-RATA ALLOCATION
1997	\$43.12	\$63.70	\$107.65
1998	\$34.34	\$50.70	\$85.68
1999	\$23.76	\$35.10	\$59.32
2000	\$17.74	\$26.20	\$44.28
2001	\$14.52	\$21.50	\$36.34
2002	\$12.53	\$18.50	\$31.27
2003	\$11.52	\$16.00	\$27.04
2004	\$10.76	\$14.10	\$23.83

The increase in licensing costs under a unified pool can be derived by subtracting *RateActual* in the first column from either *RatePC* or *RatePP*, depending on which royalty-division formula one wishes to consider in the hypothetical. The result is *RatePremium*, defined earlier in Equation 4.

Turning to transaction costs, in 2017 Robert Merges and I gathered financial data from the largest patent pool administrators in the United States that can be directly applied to this estimate. Based on our findings, the average licensee incurs about \$35,000 in costs per year dealing with a patent pool.²⁸³ These amounts stem from administrative fees tied to reporting sales data, making royalty payments, and the like.²⁸⁴ (The patent pool eliminates negotiation and search costs.) This example assumes that licensees incur similar ongoing transaction costs when working with individual outsider licensors. Added to this, in the case of an individual outsider, is the initial cost of negotiating an agreement. A widely-cited estimate suggests the average cost of an average patent licensing would be about “\$50,000 per licensee per patent.”²⁸⁵ The evidence revealed in this Article suggests the amount might be lower, however, as a pool effectively places a ceiling on the negotiations, which could simplify the process. An annual cost can be estimated by dividing this upfront negotiation cost over some period of time during which the patent has commercial value. If one assumes that period of time to be ten years, for instance, the average annual cost is \$5,000. To keep the estimate conservative, however, we may assume a higher value of, say, \$15,000. In summary, this example assumes that a licensee spends an average of \$35,000 in transaction costs for each pool it licenses from and approximately \$50,000 in transaction costs working with one outside licensor.²⁸⁶

Applying these numbers to the DVD example, one may assume, conservatively, that each licensee incurred about \$120,000 in annual administrative costs to work with two patent pools and one outsider (i.e., \$35,000 in costs for one pool, plus \$35,000 for a second pool, plus \$35,000 in administrative costs of dealing with the outsider, plus an initial cost of \$15,000 in negotiation costs with the outsiders). Under a unified pool, the annual cost would drop to \$35,000. Referring to Equation 4, the total annual transaction costs saved (*TCostsSaved*) would be approximately \$85,000.

283. See Merges & Mattioli, *supra* note 15, at 322–23.

284. See *id.*

285. Mark A. Lemley, *Rational Ignorance at the Patent Office*, 95 NW. U. L. REV. 1495, 1507 (2001) (“[A] reasonable estimate of the cost of negotiating a license might be \$50,000 per licensee per patent.”).

286. It is important to emphasize that, industry-wide, patent pools *profoundly* reduce transaction costs by reducing the number of necessary transactions and negotiations. See Merges & Mattioli, *supra* note 15, at 320.

To compare the annual transaction costs conserved to the higher rate discussed earlier and defined in Equation 4, it is necessary to estimate the total annual costs that a licensee might incur under the higher rate. (Until now, this discussion has discussed the rate in terms of per-unit sales). One can develop a ballpark figure by multiplying the *RatePremium* number by the total number of units that a licensee might expect to sell each year. Publicly available sales data reported in Form 10-K filings and annual reports makes it possible to draw such an estimate for an average licensee. In the year 2001, for instance, Sony reported selling thirty-nine million DVD players.²⁸⁷ In the interest of keeping the estimate conservative, however, one can consider *far* lower average sales numbers. Table 6, below, assumes an annual average sales figure of just one million units during the relevant years.

Table 6: Calculation of Annual Outsider Premium (based on average annual sales of 1,000,000 units)

YEAR	OUTSIDER PREMIUM (ADDITIONAL TOTAL COST TO LICENSEE UNDER UNIFIED POOL)	TCOSTSSAVED (ANNUAL)	RATE PREMIUM (PER-SALE)	RATE PREMIUM (BASED ON ANNUAL AVERAGE SALES OF 1M UNITS)
1997	\$20.48M	\$90,000	\$20.58	\$20.58M
1998	\$16.26M	\$90,000	\$16.36	\$16.36M
1999	\$11.24M	\$90,000	\$11.34	\$11.34M
2000	\$8.36M	\$90,000	\$8.46	\$8.46M
2001	\$6.88M	\$90,000	\$6.98	\$6.98M
2002	\$5.87M	\$90,000	\$5.97	\$5.97M
2003	\$4.38M	\$90,000	\$4.48	\$4.48M
2004	\$3.24M	\$90,000	\$3.34	\$3.34M

These calculations indicate that licensees should far prefer the current environment, in which they must license from two pools and one licensor, to the hypothetical setting where one pool has lured in all outsiders with higher royalties. This conclusion is directly at odds with warnings that some industry

287. See SONY CORP., SONY CORPORATION ANNUAL REPORT 2001 at 39 (2001), www.sony-latin.com/corporate/SOLA/acerca/infocorporativa/pdf/info_financiera/ar2001e.pdf [https://perma.cc/M5HF-2YV9].

analysts gave at the time fragmentation in the DVD licensing landscape occurred.²⁸⁸

In summary, the small outsider margin, multiplied across a pool in the manner pools commonly distribute royalties, leads to a significant price difference for licensees. If one assumes that a single pool would need to merely offer outsiders an amount *equal to* what they can collect outside of the pool and if one also assumes that such a pool would rely upon a commonly used basis for the division of royalties (as opposed to disproportionately compensating the outsider), the result could mean much higher rates than licensees currently pay. Outsiders may not be powerful, but multiplication is.

C. THE VIRTUES OF IMPERFECT COOPERATION

The foregoing suggests a provocative idea with implications that reach beyond patent markets: partial cooperation may, in some settings, be preferable to complete cooperation. In the context of patent pools, this condition is met when the marginal premium charged by an outsider multiplied according to the royalty-sharing rules in a pool (to lure in the outsider) exceeds the transaction costs that licensees would save by dealing with a single licensor. The case of DVD patent licensing appears to meet these conditions. This does not reflect the power of outsiders but rather that of modest arithmetic: multiplied across a pool according to the most commonly used royalty-division formulas, the small outsider margin can yield a significant total price increase.

It would be a mistake to conclude that robust patent pools that contain many essential patents are not extremely helpful. To the contrary, as discussed earlier, Robert Merges and I have estimated that the average transaction cost savings of a modern patent pool is on the order of \$400 to \$600 million.²⁸⁹ The foregoing discussion presumes a partially integrated pool taking steps to draw in a reluctant outsider. The takeaway is that the benefits pools offer are not lost or even undermined simply because an outside licensor also exists. Assuming no independent competitive concerns exist, regulators should assume that the patents that are within pools belong there, and the patents held by outsiders are not a cause for concern. By setting a baseline for outside negotiations, pools prevent these outsiders from upsetting the careful balance the pools set for their members and licensees. The fact that some patent holders prefer not to join a central pool is not necessarily a bad thing—not for licensees, not for other patent holders, and not for the pool. Antitrust

288. See *Sony, Philips Break Ranks, Prepare DVD Licensing Fees*, OPTICAL MEMORY NEWS, Aug. 13, 1996 (“The price of digital videodisk (DVD) technology may balloon if other patent holders follow the lead of Sony Electronics and Philips Electronics NV and set licensing fees for their DVD patents, warn industry analysts.”).

289. See Merges & Mattioli, *supra* note 15, at 322.

regulators concerned by recent scholarship on patent pool outsiders should consider this in their evaluation of patent pools.

Scholars in other areas of law and policy might take something away from this too. Contrary to conventional wisdom, there may exist in any given market for complementary rights an optimal level of diffusion of ownership. Jonathan Barnett has explored this concept at a high theoretical level in a compelling and thought-provoking 2009 article.²⁹⁰ Somewhere between the ideal of a grand coalition and the proverbial anticommons, there may exist middle positions where partial coalitions work alongside outsiders, subtly influencing one another in ways that are helpful or even optimal for all involved. These settings may superficially look messy and plagued by disagreements. As this study has shown, however, looks can be deceiving.

V. CONCLUSION

This Article has examined a question fundamental to law and policy: how do individuals who decline to join cooperative groups affect the good those groups can do? In the context of patents, this is a deeply important question because it challenges the belief that regulators have shaped their policies around—i.e., that patent holders can privately remedy the high transaction costs that pervade technology licensing.

Antitrust regulators have long assumed that outsider patent holders that decline to join pools do not disrupt the benefits that patent pools offer. Against this backdrop, a rising chorus of critics has theorized compellingly that outsiders are more harmful than regulators assume. By demanding royalty rates that far exceed those requested by the pool, these theorists argue, outsiders quietly undermine the transaction cost savings the pool delivers to licensees. As the theorists see it, outsiders work both sides of the deal, demanding high royalties from licensees while at the same time pressuring pools for a healthier cut of the profits. This theory suggests that the mere presence of an outsider of multiple pools should cast doubt on the efficiencies and benefits that a pool under examination can offer.

By applying an ethnographic approach, this Article has revealed an intimate and surprising look at the reality of this situation. The most important finding is that outsiders are not as powerful as the theorists have guessed. This is because the royalty rate charged by a patent pool is a powerful signal to those outside of the pool (including courts) of the reasonable value of all patents concerned.

290. See generally Jonathan M. Barnett, *Property as Process: How Innovation Markets Select Innovation Regimes*, 119 YALE L.J. 384, 387–91, 432–37 (2009).

Meanwhile, it seems that licensees are willing to resist and defy outside licensors that ask for rates far out of step with a prominent pool. As research subjects explained, some licensors work independently because they are highly motivated to “get their money fast.”²⁹¹ These licensors are understandably eager to avoid the delays and costs of pursuing a patent infringement suit against a licensee. Moreover, suing for infringement in this context can be risky: as the Lucent episode shows, an aggressive outsider strategy can backfire, leading to validity challenges and counterclaims for infringement. As one subject explained, being an outsider can also lead to negative press that a company might prefer to avoid.²⁹² Added to this is the relative difficulty of obtaining an injunction, even when infringement is found. The general view shared by subjects is that courts will tend to look to a patent pool for a ballpark sense of the value of the patents infringed. It is no wonder that the licensing rates charged by outsiders in the DVD and MPEG-2 episodes were roughly in line with those of the pools they operated alongside.

The impetus to keep royalties reigned-in is even stronger for outside patent holders who are also licensees of a pool. As the DVD study shows, Thomson (a manufacturer) was highly successful in conducting outside licenses overall, but it lowered its asking price when making deals with patent holders whose patents it wished to license. A patent pool that includes a grant-back clause for licensees would make this a contractual obligation.

Finally, an outside licensor who, despite these many countervailing forces, succeeds in getting licensees to agree to pay a high rate still must contend with underreporting of sales. As research subjects explained, underreporting is common (it is costly to monitor and detect), and it tends to nudge payments from licensees to outsiders to be in line with pool rates.

The examination of royalty rates and prices in Part III brings these findings into stark relief. The data analyzed support the qualitative insights shared by research subjects: the per-patent-family rates charged by two pools and one independent licensor were all within a similar range. Moreover, to bring all patent holders in, a single pool may have had to raise its royalty rates in a manner that would have resulted in an overall price increase for licensees. This is not because the outsider advantage is large, but rather, because of how pools divide royalties: the small margin needed to draw in an outsider, multiplied across a pool in the manner pools usually distribute royalties, leads to a significant difference in price. The existing licensing landscape, imperfect as it might seem, may be more desirable than more aesthetically pleasing alternatives.

291. Telephone Interview with Subject #8 (July 15, 2017).

292. *Id.*

Putting this all together, cooperation among patent holders is not an *all-or-nothing* game. Contrary to theory, outsiders and secondary pools do not appear to undermine the benefits that patent pools offer. This is because patent pools have a quiet but powerful influence on negotiations that take place “poolside,” so to speak. This is why the gentle fragmentation among licensors that pervades technology licensing is mostly harmless, probably inevitable, and sometimes actually preferable to the alternative. Antitrust regulators who must evaluate patent pools should find this knowledge helpful. This finding can also be helpful to scholars concerned by outsider problems in many other areas of law and policy. An ethnographic approach like the one followed here can reveal aspects of an outsider situation that theory alone does not capture. Sometimes, the collective will of a group overpowers individual self-interest; sometimes, an outsider is also a good neighbor; sometimes, a little cooperation is not only better than none, but also better than more.

THE RIGHT TOOLS: EUROPE’S INTERMEDIARY LIABILITY LAWS AND THE EU 2016 GENERAL DATA PROTECTION REGULATION

Daphne Keller[†]

ABSTRACT

The European Union’s (EU) General Data Protection Regulation (GDPR) makes important changes to the “Right to Be Forgotten” established by the Court of Justice of the European Union’s landmark 2014 *Google Spain* ruling. The GDPR introduces new notice-and-takedown rules for “Right to Be Forgotten” requests that will make deliberate or accidental over-removal of online information far too likely. The new rules give private Internet platforms powerful incentives to erase or delist user-generated content—whether or not that content, or the intermediaries’ processing of the content, actually violates the law. These problems could be mitigated, without threatening the important privacy protections established by the GDPR, through procedural checks and balances in the platforms’ removal operations.

This Article details the problematic GDPR provisions, examines the convergence of European data protection and intermediary liability law, and proposes ways that the EU’s own intermediary liability laws can restore balanced protections for privacy and information rights. The Article focuses on the motivations and likely real-world behavior of online platforms. It includes close examinations of:

- Whether and how the “Right to Be Forgotten” may apply to user-generated content hosts like Twitter or Facebook;
- Free expression provisions in the GDPR;
- The GDPR’s extraterritorial reach and consequences for companies outside the EU;
- Doctrinal tensions between the EU’s intermediary liability law under the eCommerce Directive and the EU’s data protection law under the 1995 Data Protection Directive and the new GDPR; and
- Human rights and fundamental rights laws governing online notice-and-takedown operations.

DOI: <https://doi.org/10.15779/Z38639K53J>

© 2018 Daphne Keller.

[†] Daphne Keller is the Director of Intermediary Liability at Stanford Law School’s Center for Internet and Society. She was previously Associate General Counsel for Intermediary Liability at Google. In that role, she worked closely with the independent Advisory Council convened by Google to advise the company on its RTBF obligations and had the opportunity to listen to and speak with many of Europe’s leading thinkers on data protection. She would like to thank the many people who lent their time and expertise to strengthen the Article, including John Bowman, Neal Cohen, David Erdos, Peter Fleischer, Al Gidari, Jennifer Granick, Jim Greer, Joris van Hoboken, Chris Kuner, Harjinder Obhi, Miquel Peguera, and Michel José Raymond. Mistakes are hers and not theirs.

TABLE OF CONTENTS

I.	INTRODUCTION	289
A.	ISSUE OVERVIEW	290
B.	USING THIS ARTICLE AS A TOOLKIT.....	293
II.	CONVERGENCE OF LEGAL FRAMEWORKS	294
A.	INTERMEDIARY LIABILITY HISTORY AND LAW.....	294
B.	DATA PROTECTION HISTORY AND LAW	305
C.	DATA PROTECTION AND ONLINE SERVICE PROVIDERS	308
D.	THE <i>GOOGLE SPAIN</i> RULING	312
E.	THE 2016 GENERAL DATA PROTECTION REGULATION.....	317
III.	THREATS TO INTERNET USERS' RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION	319
A.	UNCLEAR RULES AND ONE-SIDED INCENTIVES	320
B.	RIGHT TO BE FORGOTTEN OBLIGATIONS FOR HOSTS AND SOCIAL MEDIA.....	322
C.	NOTICE-AND-TAKEDOWN PROCESS	327
1.	<i>Removal Requests</i>	329
2.	<i>Temporarily "Restricting" Content</i>	330
3.	<i>Permanently "Erasing" Content</i>	332
4.	<i>Transparency</i>	335
D.	FREE EXPRESSION AND INFORMATION PROTECTIONS.....	341
1.	<i>Express General Data Protection Regulation Provisions</i>	341
2.	<i>Enforcement Processes</i>	343
E.	JURISDICTION	347
1.	<i>Prescriptive Jurisdiction: Who Must Comply?</i>	348
2.	<i>Territorial Scope of Compliance: Must OSPs Erase Content Globally?</i>	349
IV.	RELATION TO NOTICE-AND-TAKEDOWN RULES OF THE ECOMMERCE DIRECTIVE	351
A.	PROCEDURAL PROTECTIONS FOR INFORMATION RIGHTS UNDER THE ECOMMERCE DIRECTIVE.....	351
B.	APPLICABILITY OF THE ECOMMERCE DIRECTIVE TO RTBF REMOVALS.....	354
1.	<i>Conceptual Tensions Between Intermediary Liability and Data Protection</i>	354
2.	<i>Confusing Language in the Governing Instruments</i>	356
3.	<i>Reconciling the eCommerce Directive and Data Protection Law</i>	358
V.	SOLUTIONS	361
A.	RULES FROM THE ECOMMERCE DIRECTIVE SHOULD GOVERN NOTICE-AND-TAKEDOWN UNDER THE GDPR	361

B.	IF GDPR RULES APPLY TO NOTICE-AND-TAKEDOWN, THEY SHOULD BE INTERPRETED TO MAXIMIZE PROCEDURAL FAIRNESS	362
C.	HOSTS SHOULD NOT BE SUBJECT TO RTBF OBLIGATIONS.....	362
D.	DPAS SHOULD NOT ASSESS FINANCIAL PENALTIES AGAINST OSPs THAT REJECT RTBF REQUESTS IN GOOD FAITH	363
E.	EU MEMBER STATE LAW AND REGULATORY GUIDANCE SHOULD ROBUSTLY PROTECT FREEDOM OF EXPRESSION IN RTBF CASES	363
F.	JURISDICTIONAL RULES SHOULD RESPECT NATIONAL LEGAL DIFFERENCES.....	363
VI.	CONCLUSION	364

I. INTRODUCTION

Internet technologies have vastly expanded access to information and opportunities for free expression around the world. At the same time, they have posed unprecedented threats to individual privacy. These two developments—and the underlying human rights affected by them—came into conflict with the Court of Justice of the European Union’s (CJEU) *Google Spain* ruling, which established the doctrine popularly called the “Right to Be Forgotten” (RTBF).

Google Spain also surfaced tensions between two strikingly different areas of law, both of which shape Internet users’ rights online. The first area of law, intermediary liability, focuses on the legal responsibility that Online Service Providers (OSPs) have for their users’ speech. It is a key source of protection for individual expression and information rights on the Internet. The second, data protection, focuses on information about individual people. It gives them legal rights to limit the ever-proliferating uses of their personal data, both online and off. Both sets of laws protect fundamental rights and preserve Internet services as, in the words of the European Court of Human Rights (ECHR), “essential tools for participation” in contemporary society and public life.¹ But these laws do so through profoundly different legal frameworks.

Tensions between intermediary liability and data protection persist in the EU’s major new data protection law—the General Data Protection Regulation (GDPR). In provisions that have gone largely unexamined, the GDPR subtly reshapes the RTBF. This Article examines troubling consequences of these

1. *Yildirim v. Turkey*, App. No. 3111/10, Eur. Ct. H.R. ¶ 54 (2012), <http://hudoc.echr.coe.int/fre?i=001-115705> [<https://perma.cc/E6AW-KBDL>].

new provisions and suggests tools of European law that can be used to better balance the rights affected.

A. ISSUE OVERVIEW

Data protection and intermediary liability laws came together with a bang when the CJEU endorsed a so-called “Right to Be Forgotten” under EU data protection law. In *Google Spain*, the CJEU ruled that Google must honor a claimant’s request to exclude certain search results when users search for the claimant’s name.² The right that the court established, which might more accurately be termed a right to “delist” information from search engines, was not absolute. The claimant’s rights had to be balanced against those of other people, including other Internet users looking for information online.³ Rather than have European courts strike this balance on a case-by-case basis, the CJEU placed de facto adjudication power in the hands of Google, requiring the company to assess each delisting request and decide whose rights should prevail.⁴

The legal obligations created by *Google Spain* have been well examined in the academic, popular, and professional literature.⁵ But these obligations changed in May of 2018, when the EU’s new General Data Protection Regulation (GDPR) went into effect. The GDPR brings an enhanced RTBF to Europe and, through expansive jurisdiction provisions, to the rest of the world.⁶

2. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317.

3. *Id.* ¶ 97.

4. *Id.*

5. See, e.g., Aleksandra Kuczerawy & Jef Ausloos, *From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain*, 14 COLO. TECH. L.J. 219, 226 (2016); Stefan Kulk & Frederik Zuiderveen Borgesius, *Google Spain v. González: Did the Court Forget About Freedom of Expression?*, 5 EUR. J. RISK REG. 389, 390–92 (2014); Miquel Peguera, *The Shaky Ground of the Right to Be Delisted*, 18 VAND. J. ENT. & TECH. L. 507, 539 (2016); Joris van Hoboken, Case Note, CJEU 13 May 2014, C-131/12 (*Google Spain*) (Aug. 15, 2014) (unpublished manuscript), <https://ssrn.com/abstract=2495580> [<https://perma.cc/93P7-XXXE>]; Christopher Kuner, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges*, in PROTECTING PRIVACY IN PRIVATE INTERNATIONAL AND PROCEDURAL LAW AND BY DATA PROTECTION 19 (Burkhard Hess & Cristina M. Mariottini eds., 2015); Farhad Manjoo, *‘Right to Be Forgotten’ Online Could Spread*, N.Y. TIMES (Aug. 5, 2015), www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html [<https://perma.cc/XU4Y-6SX2>].

6. Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]; see also generally *Reform of European Data Protection Rules*, EUROPEAN COMM’N, https://ec.europa.eu/info/law/law-topic/data-protection/reform_en [<https://perma.cc/E7JN-9HGZ>] (last visited Mar. 31, 2018).

As this Article will discuss, the GDPR locks in language and processes rooted in data protection laws that fit poorly with OSPs' function as platforms for communication. The GDPR couples unclear RTBF obligations for OSPs with unusually powerful compliance incentives—including potential fines as high as four percent of annual global turnover or twenty million euros.⁷ Unless lawmakers establish rules or guidelines limiting the law's impact, OSPs will have good reason to honor not only legitimate RTBF requests, but also abusive or mistaken ones, and will remove information the European public has every right to see. Overreaching RTBF requests that Google has already reported receiving include: claims from public officials trying to suppress old criminal records, priests wanting to disguise a history of sexual abuse in their parishes, and financial professionals attempting to hide convictions for defrauding clients.⁸ Both Google and Bing report that over half of the delisting requests they receive state claims that, like these examples, are not valid requests for removal under European laws.⁹

This pattern of overreaching requests should come as no surprise. Abusive removal demands are a problem whenever OSPs, ranging from Internet infrastructure providers to major social media sites, operate “notice-and-takedown” systems, under which claimants submit legal notices or requests for removal of online expression. Studies suggest that OSPs comply with legally baseless requests all too often.¹⁰ No matter what one thinks about the proper scope of legitimate delisting or removal requests, the abusive ones are a problem. Relying on technology companies to resolve delicate questions of law

7. GDPR, *supra* note 6, art. 83(5). As discussed in *infra* Section III.A, more sophisticated OSPs will likely be advised to expect far lower fines, but most OSPs will not have access to such expert advice.

8. *See generally Transparency Report*, GOOGLE, <https://transparencyreport.google.com/privacy/overview> [<https://perma.cc/RE94-7QKE>] (last visited Mar. 31, 2018); Mischee Smith, *Updating Our “Right to Be Forgotten” Transparency Report*, GOOGLE (Feb. 26, 2018), <https://www.blog.google/topics/google-europe/updates-our-right-to-be-forgotten-transparency-report> [<https://perma.cc/388V-JG3A>]; THEO BERTRAM ET AL., GOOGLE, *THREE YEARS OF THE RIGHT TO BE FORGOTTEN* (2018), <https://drive.google.com/file/d/1H4MKNwf5MgezG7OnJRnl3ym3gIT3HUK> [<https://perma.cc/J274-LA7B>] (providing detailed quantitative reporting on sources, types, and outcomes of RTBF requests).

9. *Id.*; *Content Removal Requests Report*, MICROSOFT, <https://www.microsoft.com/en-us/about/corporate-responsibility/crrr> [<https://perma.cc/5Q49-JVYX>] (last visited Mar. 31, 2018). DPAs reviewing delisting claims rejected by the companies concluded that “in the great majority of cases the refusal by a search engine to accede to the request is justified . . .” Press Release, Article 29 Data Prot. Working Party, Issued by the Article 29 Data Protection Working Party (June 18, 2015), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20150618_wp29_press_release_on_delisting.pdf [<https://perma.cc/5TEN-J7A5>]. This suggests that the self-reported rate of improper requests is roughly accurate by regulators' standards. *See id.*

10. *See infra* Section II.A.

that affect Internet users' fundamental rights is also a problem, particularly for laws that vary from country to country. But they are not new problems, nor intractable ones. They arise over and over in the context of intermediary liability law. Europe's own existing intermediary liability laws, along with guidance from human rights bodies and civil society institutions, provide tools to solve them.¹¹ In particular, procedural rules for notice-and-takedown operations can, like procedural rules in litigation, make the process fairer for all sides and increase the likelihood of just outcomes.

This Article is about using those tools to help the GDPR achieve its real goals: balancing and protecting *all* rights, including both privacy and information rights. It will closely examine the GDPR's new notice-and-takedown rules and argue that they are, on their face, dangerous to information rights, expression rights, and to the Internet as an open platform for democratic participation. The GDPR, however, can perhaps be interpreted in light of fundamental rights considerations to arrive at a more balanced set of rules. The Article presents a proposed analysis for practitioners and lawmakers seeking to do so.

It is also important to note, at the outset, that this Article is emphatically not about two other, related issues.

First, this Article is not about the underlying substantive legal right to “be forgotten” by obscuring or erasing truthful information about oneself. This Article does not take the position that such laws are good or bad. Every legal system has laws that limit expression rights to protect privacy, and vice versa. Advocating for a particular version of this difficult balance is not the Article's point. Instead, this Article focuses on procedural fairness. Without well-designed notice-and-takedown rules, national laws balancing privacy and free expression will not be enforced. OSPs considering removal requests will always have reason to privilege privacy over expression, and to delete more than the law requires.

Second, this Article is not about the data that OSPs collect by tracking their own users' online behavior. OSPs have plenty of this privately held, “back-end” data—logs tracking users' clicks, profiles used to target advertisements, and more. Data protection laws, including erasure obligations, rightly apply to this back-end data. This Article does not dispute Internet users' rights under the GDPR to make OSPs erase data of this sort. Accordingly, the term “RTBF” as used in this Article will only refer to the right to erase or delist information put online by another Internet user.

11. See Kuczerawy & Ausloos, *supra* note 5, at 233 (“The lessons learned in the ongoing discussions on notice-and-takedown could inform the development of procedural safeguards in the context of the right to be delisted.”).

Discussions of the RTBF all too often lead to miscommunication between well-meaning people on all sides of the issue. In particular, specialists in intermediary liability and specialists in data protection may bring disparate assumptions and vocabularies to the topic. This Article seeks to bridge that divide, and to identify doctrinal and principled intersections of the two approaches. By drawing on the strengths of both perspectives, policymakers can devise approaches to Internet technologies that respect both privacy and information rights.

B. USING THIS ARTICLE AS A TOOLKIT

This Article tackles big questions. What is the proper role for private platforms in resolving conflicts between Internet users' privacy and information rights? If private companies must resolve such disputes, how can lawmakers promote fair outcomes? What should happen when different countries reach different answers to these questions? To suggest resolutions, the Article plumbs the depths of two rather technical areas of law: data protection and intermediary liability. The Article is drafted for maximum practical value to the practitioners, policymakers, and thinkers who will grapple with the RTBF under the GDPR. Its structure is deliberately modular, with a detailed table of contents to let busy readers skip directly to relevant Parts and Sections. The goal is to provide a legal toolkit supporting balanced protections for both privacy and free expression rights online.

Beginning in Part II, the Article will review the history of data protection and intermediary liability law, their convergence in the RTBF, and the emergence of the EU's momentous new law—the GDPR. Part III will detail the GDPR provisions that affect publicly shared online information and expression. It includes a careful overview of the law's problematic notice-and-takedown procedural rules. Part IV will suggest a way to avoid those rules entirely, by invoking the EU's primary intermediary liability law—the eCommerce Directive—along with European courts' rulings connecting that law to fundamental rights.¹² Applying the eCommerce Directive in the data protection context would require the resolution of longstanding, but not insoluble, doctrinal disputes.

Each problematic provision of the GDPR comes with an opportunity to advance better interpretations. The law's ambiguity is in this sense an asset, because it creates an opening to seek better and more balanced readings. Part V of the Article will list stand-out opportunities to do so. Specifically, it will recommend:

12. Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC) [hereinafter eCommerce Directive].

1. Relying on rules based on the eCommerce Directive and fundamental rights considerations, rather than the GDPR, to govern notice-and-takedown procedures.
2. Interpreting individual GDPR provisions to mitigate the threats they pose to Internet users' rights, including both expression and privacy rights.
3. Limiting RTBF obligations to search engines such as Google or Bing, and not extending them to hosting platforms, such as Twitter or DailyMotion.
4. Encouraging OSPs to protect their users' expression, information, and privacy rights in response to RTBF requests by guaranteeing that the OSPs will not face financial penalties for doing so.
5. Adopting stronger express protections for information and expression rights.
6. Only requiring OSPs to honor RTBF requests in countries where doing so is consistent with national law.

In sum, this Article will suggest ways that European policymakers can protect online privacy and data protection rights, using existing European legal tools, without unnecessarily harming information and expression rights in the process.

II. CONVERGENCE OF LEGAL FRAMEWORKS

The law of data protection and the law of intermediary liability have been on a collision course for a long time, but cases squarely raising the two issues have emerged only recently. Historically, few lawyers needed to draw a connection between the two fields. Each uses a distinct vocabulary and is for the most part interpreted, enforced, and litigated by different practitioners. A lawyer who views an issue through the lens of intermediary liability and one who views the same issue through the lens of data protection may have trouble even understanding each other's concerns. The following Sections will review the history of the two fields and their eventual convergence, first in *Google Spain* and then in the GDPR.

A. INTERMEDIARY LIABILITY HISTORY AND LAW

The law of intermediary liability limits OSPs' legal responsibility for user activities and effectively protects individual Internet users' rights to seek and impart information.

Major intermediary liability laws include the Digital Millennium Copyright Act (DMCA) in the United States and the eCommerce Directive in the EU.¹³ Both immunize intermediaries, such as cable or mobile Internet access providers, caching providers, and hosts that provide storage and display services, from liability for user-generated content.¹⁴ As a general matter, these laws immunize OSPs that engage in standard technical operations required as part of their service to users. OSPs may be liable, however, when they have more active, conscious engagement with the content—if OSPs themselves author material, or assume practical responsibility for material posted by users, they may lose the immunity.¹⁵ OSPs are also typically liable if they knew or should have known about unlawful content and failed to act.¹⁶ OSPs often operate notice-and-takedown systems so that claimants can notify them about content that should be removed.¹⁷ By removing unlawful content upon notice, OSPs can preserve so-called “safe harbors” or immunities from claims regarding the content. For large companies, notice-and-takedown operations may include standardized intake forms for notices, legal teams dedicated to handling them, and specialized tools to track and act upon them.¹⁸ Smaller companies may have simpler systems or respond to take-down requests ad hoc.¹⁹

Intermediary liability laws protect users’ rights by reducing the incentives OSPs would otherwise have to interfere with users’ expression and access to information. Without immunities, liability concerns could lead OSPs to build only “walled garden” platforms, which exclude the general public and expose

13. 17 U.S.C. § 512 (2012); eCommerce Directive, *supra* note 12, arts. 12–15.

14. *See* 17 U.S.C. § 512 (2012); eCommerce Directive, *supra* note 12, arts. 12–15.

15. *See, e.g.*, Case C-324/09, L’Oréal SA v. eBay Int’l AG, 2011 E.C.R. I-6011, ¶ 6 (holding that an online marketplace may lose immunity under the eCommerce Directive where it actively optimizes or promotes particular offers of sale); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 40 (2d Cir. 2012) (explaining that an OSP might lose immunity for manually selecting user-generated videos for syndication to a third party).

16. eCommerce Directive, *supra* note 12, art. 14(1)(a) (providing knowledge-based liability for hosts in the EU); 17 U.S.C. § 512(c)(1)(A) (2012) (providing knowledge-based liability for copyright claims against hosts in the United States). *But see* 47 U.S.C. § 230(c)(2), (e)(2) (2012) (providing OSPs with complete immunity for most non-intellectual property civil claims).

17. *See, e.g.*, *Removing Content from Google*, GOOGLE, <https://support.google.com/legal/troubleshooter/1114905?hl=en> [<https://perma.cc/4BVE-PQLE>] (last visited Mar. 31, 2018); *Submit a Request*, MEDIUM, https://help.medium.com/hc/en-us/requests/new?ticket_form_id=165717 [<https://perma.cc/6LTT-7EHZ>] (last visited Mar. 31, 2018).

18. *See supra* note 17.

19. *See* JENNIFER M. URBAN ET AL., NOTICE AND TAKEDOWN IN EVERYDAY PRACTICE (2017), <https://ssrn.com/abstract=2755628> [<https://perma.cc/K2LF-NTBL>].

users only to content that the OSP selects.²⁰ At the same time, OSPs would have reason to over-police and remove controversial but legal expression shared by users.

Intermediary liability law sits at a unique and often troubling intersection of state and private power. When OSPs remove user expression based on actual or perceived legal requirements, the harm to the user's rights can be traced to state action through laws which create OSP liability. Removals motivated by fear of liability are in this sense different from the ones many OSPs carry out based on their own community guidelines or terms of service.²¹ Voluntary content removals also affect online expression and are rightly scrutinized by Internet rights advocates. But they typically do not raise the specter, key to intermediary liability law, of "collateral censorship" based on state action. As Yale Law Professor Jack Balkin explains,

Collateral censorship occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B's speech. This will lead A to block B's speech or withdraw infrastructural support from B. In fact, because A's own speech is not involved, A

20. See *AOL's 'Walled Garden'*, WALL ST. J. (Sept. 4, 2000, 11:57 PM), www.wsj.com/articles/SB968104011203980910 [<https://perma.cc/8STK-C8RN>].

21. State action can, of course, also affect OSPs' nominally voluntary removal decisions. When it does, state human rights obligations may be implicated. See *Backpage.com, LLC v. Dart*, 807 F.3d 229 (7th Cir. 2015) (holding that a sheriff violated the First Amendment by pressuring credit card companies to terminate service to a website based on the website's offensive but lawful activity); DOUWE KORFF, COUNCIL OF EUROPE, *THE RULE OF LAW ON THE INTERNET AND IN THE WIDER DIGITAL WORLD* 23 (2014), <https://rm.coe.int/16806da51c> [<https://perma.cc/46N2-CSLV>] (listing Council of Europe Human Rights Commissioner's recommendation that member states "stop relying on private companies that control the Internet and the wider digital environment to impose restrictions that are in violation of the state's human rights obligations" and discussing states' responsibilities to limit even "measures implemented by private parties for business reasons, without direct involvement of the state"); COUNCIL OF EUROPE & SWISS INST. OF COMPARATIVE LAW, *COMPARATIVE STUDY ON BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT* 21–22 (2015), <http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet> [<https://perma.cc/56FK-W2ZY>] (summarizing arguments for liability of private OSPs for voluntary removals or liability of governments for permitting such removals); CHRISTINA ANGELOPOULOS ET AL., *STUDY OF FUNDAMENTAL RIGHTS LIMITATIONS FOR ONLINE ENFORCEMENT THROUGH SELF-REGULATION* 50–51 (2016), <http://www.ivir.nl/publicaties/download/1796> [<https://perma.cc/8QAW-79QT>]; Aleksandra Kuczerawy, *The Power of Positive Thinking: Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression*, 8 J. INTELL. PROP. INFO. TECH. & E-COM. L. 226 (2017).

has incentives to err on the side of caution and restrict even fully protected speech in order to avoid any chance of liability.²²

Intermediary liability protections allow private platforms to support public participation and expression at a scale never dreamed of pre-Internet. If YouTube had to manually review all four hundred hours of video users upload each minute, for example, its operations would be impossible and the Internet would lose an important speech platform.²³ Well-designed intermediary liability laws are essential to make open platforms, and the speech they enable, possible.

At the same time, intermediary liability laws can mitigate another problem for online expression: OSPs' incentives to remove any controversial or legally questionable speech. Anecdotal evidence and academic studies show that OSPs receive many inaccurate or bad faith removal requests—and, too often, comply with them.²⁴ For example, scholars reviewing Google's U.S. copyright-

22. Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2309 (2014). In unusual cases, economic incentives may weigh against removal. For ordinary user speech on large-scale platforms, however, liability risk is the biggest financial consideration. Minimizing such risk could even be seen as a fiduciary duty to shareholders.

23. See Sirena Bergman, *We Spend a Billion Hours a Day on YouTube, More than Netflix and Facebook Video Combined*, FORBES (Feb. 28, 2017, 7:32 AM), www.forbes.com/sites/sirenabergman/2017/02/28/we-spend-a-billion-hours-a-day-on-youtube-more-than-netflix-and-facebook-video-combined/ [<https://perma.cc/7JWS-9E9P>] (reporting that YouTube receives “around 400 hours of content every minute, from creators all over the world”). Automated filters can speed up content review, but introduce important errors. For example, YouTube has repeatedly taken down videos archived by activists to document human rights abuses. See, e.g., Malachy Browne, *YouTube Removes Videos Showing Atrocities in Syria*, N.Y. TIMES (Aug. 22, 2017), <https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html> [<https://perma.cc/5PEM-JSA5>]; Scott Edwards, *When YouTube Removes Violent Videos, It Impedes Justice*, WIRED (Oct. 7, 2017, 10:00 AM), <https://www.wired.com/story/when-youtube-removes-violent-videos-it-impedes-justice/> [<https://perma.cc/TZH7-GR62>]; Daphne Keller, *Problems With Filters in the European Commission's Platforms Proposal*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y (Oct. 5, 2017, 3:33 PM), <http://cyberlaw.stanford.edu/blog/2017/10/problems-filters-european-commissions-platforms-proposal> [<https://perma.cc/KQF5-DLH2>].

24. See Daniel Seng, *The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices*, 18 VA. J.L. & TECH. 369, 441 (2014) (conducting An empirical study of DMCA takedown notices and documenting “ill-informed copyright owners and reporters submitting vague, ambiguous, and abusive takedown requests”); URBAN ET AL., *supra* note 19, at 3 (“Seventy percent of the requests [for removal from Google Image Search] raised serious questions about their validity . . .”); Jennifer Urban & Laura Quilter, *Efficient Process or ‘Chilling Effects’? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA HIGH TECH. L.J. 621, 642 & 667 (2005) (reviewing all notices received by Google, and concluding that twenty-nine percent raised substantively flawed claims); Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, CTR. FOR INTERNET & SOC'Y 2 (2011), <http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf> [<https://perma.cc/G7EY-V4JG>] (describing how intermediaries empirically “over-complied”

based removals in 2006 found that almost a third of requests raised questionable legal claims.²⁵ Most data and anecdotal evidence of over-removal comes from copyright claims under the U.S. DMCA,²⁶ because of the significant volume of removals and relatively high degree of public transparency possible under that law.²⁷ Notorious examples include copyright claims attempting to remove consumer reviews,²⁸ Wikipedia articles,²⁹ major news sources,³⁰ and content licensed by the accuser.³¹ Abusive DMCA requests

with takedown notices, despite the notices' questionable validity); Christian Ahlert et al., How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation 11 (unpublished manuscript), <http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf> [<https://perma.cc/8TCF-3QPR>] (last visited Mar. 31, 2018) (explaining how “companies engage in a form of commercial war on the internet” using removal requests, by “putting bad faith claims against their competitor’s Web content”); John Leyden, *How to Kill a Website with One Email: Exploiting the European E-Commerce Directive*, REGISTER (Oct. 14, 2004, 8:38 AM), www.theregister.co.uk/2004/10/14/isp_takedown_study/14/isp_takedown_study/ [<https://perma.cc/P24V-5LJ4>] (“How much effort does it take to get an ISP to pull public domain material using unsubstantiated legal threats? Distressingly little, according to a recent study by Dutch group Bits of Freedom.”).

25. Urban & Quilter, *supra* note 24, at 666.

26. 17 U.S.C. § 512 (2012).

27. See Jennifer M. Urban et al., *Takedown in Two Worlds: An Empirical Analysis*, 64 J. COPYRIGHT SOC'Y 483, 489 (2018) (analyzing “288,675 notices containing well over 100 million (108,331,663) individual takedown requests—i.e., claims of infringement” made publicly available in the Lumen Database)

28. Eric Goldman, *The Latest Insidious Tactic to Scrub Online Consumer Reviews*, FORBES (July 23, 2013, 12:07 PM), <http://www.forbes.com/sites/ericgoldman/2013/07/23/the-latest-insidious-tactic-to-scrub-online-consumer-reviews/> [<https://perma.cc/Q6LF-EV4Q>].

29. Aaron Souppouris, *Microsoft Mistakenly Asks Google to Block the BBC, Wikipedia, US Government Webpages*, VERGE (Oct. 8, 2012, 7:50 AM), <http://www.theverge.com/2012/10/8/3472662/microsoft-dmca-takedown-bbc-wikipedia-government-google-search> [<https://perma.cc/97GM-DTTB>].

30. *Id.*

31. Zahavah Levine, *Broadcast Yourself*, YOUTUBE OFFICIAL BLOG (Mar. 18, 2010), <https://youtube.googleblog.com/2010/03/broadcast-yourself.html> [<https://perma.cc/SF9B-LCKH>] (describing Viacom’s pattern of uploading videos to YouTube for promotional purposes, then mistakenly demanding removal of the same videos, and linking to supporting litigation evidence).

have also been used to silence scientific³² and religious³³ disagreement. According to transparency reports in 2017, Twitter rejects about twenty percent of DMCA removal requests as invalid;³⁴ Tumblr rejects about fifteen percent;³⁵ and Automatic/WordPress rejects eighty-three percent.³⁶

Practitioners, scholars, and NGOs have, over time, developed expertise about ways to protect online expression against over-removal, by imposing checks and balances on the removal process. The Manila Principles, a set of notice-and-takedown rules endorsed by many Internet civil liberties organizations and human rights officials,³⁷ recommends:

- Requiring claimants to include adequate information in removal requests.³⁸

32. Ivan Oransky, *WordPress Removes Anil Potti Posts from Retraction Watch in Error After False DMCA Copyright Claim*, RETRACTION WATCH (Feb. 5, 2013, 10:00 PM), <http://retractionwatch.com/2013/02/05/wordpress-removes-anil-potti-posts-from-retraction-watch-in-error-after-false-dmca-copyright-claim/> [https://perma.cc/AHQ5-SVYL]; John Timmer, *Site Plagiarizes Blog Posts, Then Files DMCA Takedown on Originals*, ARS TECHNICA (Feb. 5, 2013, 3:33 PM), <http://arstechnica.com/science/2013/02/site-plagiarizes-blog-posts-then-files-dmca-takedown-on-originals/> [https://perma.cc/PVZ8-C5X4].

33. Eva Galperin, *Massive Takedown of Anti-Scientology Videos on YouTube*, ELEC. FRONTIER FOUND. (Sept. 5, 2008), <https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube> [https://perma.cc/85UE-DN3F].

34. *Transparency Report: Copyright Notices*, TWITTER (July–Dec. 2017), <https://transparency.twitter.com/en/copyright-notices.html#copyright-notices-jul-dec-2017> [https://perma.cc/Y47P-2EUN] (indicating that material was removed eighty percent of the time).

35. *Copyright and Trademark Transparency Report*, TUMBLR (Jan.–June 2017), https://static.tumblr.com/uhwk34h/idlp19nvc/iptransparencyreport2017b_2.pdf [https://perma.cc/E3RQ-499K] (“From January to June 2017, we received 10,837 DMCA notices and determined that 85% (9,257) were valid.”).

36. *Intellectual Property: Copyright*, AUTOMATIC/WORDPRESS (July 1–Dec. 31, 2017), <https://transparency.automatic.com/intellectual-property/2017-h2/> [https://perma.cc/TD8F-U7Q2] (indicating that seventeen percent of DMCA notices resulted in action “where some or all content was removed”).

37. See *Manila Principles on Intermediary Liability*, MANILAPRINCIPLES.ORG, <https://www.manilaprinciples.org/> [https://perma.cc/B4C3-4VC3] (last visited Mar. 31, 2018) [hereinafter MANILA PRINCIPLES]; David Kaye (Special Rapporteur), Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* at 6, U.N. Doc. A/HRC/32/38 (May 11, 2016), http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/38 [https://perma.cc/4RMF-U8EJ] (explaining that the Manila Principles “establish baseline protection for intermediaries in accordance with freedom of expression standards”); see also *Online Services, Including e-Commerce, in the Single Market*, at 44, SEC (2011) 1641 final (Jan. 11, 2012), http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf [https://perma.cc/4W52-5R8F] [hereinafter *Single Market Online Services*] (listing other model rules or guidelines from individual civil liberties organizations).

38. MANILA PRINCIPLES, *supra* note 37, art. 3(b); see also 17 U.S.C. § 512(c)(3)(A) (2012).

- Providing notice to the user whose content is alleged to violate the claimant's rights.³⁹
- Giving the accused user the opportunity to contest the accusation.⁴⁰
- Assessing fines, penalties, or damages for removal requests made in bad faith.⁴¹
- Providing public transparency about removals.⁴²
- Ensuring that OSPs are not required to actively monitor or police user content.⁴³

Procedural rules like these protect rights that are listed in the United States Constitution, and that in the EU are guaranteed under the Charter of Fundamental Rights.⁴⁴ Following European parlance, this Article refers to these as “fundamental” rights. Fundamental rights that are affected by intermediary liability laws include the rights to free expression and information access,⁴⁵ rights to privacy and data protection,⁴⁶ rights to conduct business and provide services,⁴⁷ rights to assembly and association,⁴⁸ and rights to effective remedies and fair trials.⁴⁹

39. MANILA PRINCIPLES, *supra* note 37, art. 5.

40. *Id.*

41. *Id.* art. 3(g).

42. *Id.* art. 6; *see also* Brief of Amici Curiae Chilling Effects Clearinghouse Leaders in Support of Appellee at *8–16, *Perfect 10, Inc. v. Google, Inc.*, 653 F.3d 976 (9th Cir. 2011), 2010 WL 5813411 (listing research and scholarship that depends on Lumen database (formerly known as Chilling Effects)).

43. MANILA PRINCIPLES, *supra* note 37, art. 1(d).

44. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 2 [hereinafter Charter] (listing rights including the right to free expression and information, *id.* art. 11, the right to “good administration,” *id.* art. 41, and right to an effective remedy and to a fair trial, *id.* art. 47); U.S. CONST. amends. I (listing the right to free expression), V (listing the right to due process); ANGELOPOULOS ET AL., *supra* note 21.

45. Charter, *supra* note 44, art. 11; *see also* Case C-360/10, *Belgische Vereniging van Auteurs Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, [2012] 2 C.M.L.R. 18, ¶ 48 (explaining that an OSP monitoring requirement may threaten the freedom to receive or impart information).

46. Charter, *supra* note 44, arts. 7, 8; *see also* *Netlog*, 2 C.M.L.R. 18, ¶ 48 (explaining that an OSP monitoring requirement may threaten the right to protection of personal data).

47. Charter, *supra* note 44, arts. 15, 16; *see also* *Netlog*, 2 C.M.L.R. 18, ¶ 47 (explaining that an OSP monitoring requirement may threaten the freedom to conduct business).

48. Charter, *supra* note 44, art. 12; *see also* ANGELOPOULOS ET AL., *supra* note 21, at 22, 34 (discussing assembly right).

49. Charter, *supra* note 44, art. 47; *see also* ANGELOPOULOS ET AL., *supra* note 21, at 22 (describing remedies rights); *see also* Martin Husovec, *Injunctions Against Innocent Third Parties: The Case of Website Blocking*, 4 J. INTELL. PROP. INFO. TECH. & E-COM. L. 116, 123 (2012)

The core intermediary liability law in the EU is the eCommerce Directive, enacted in 2000.⁵⁰ This EU-wide law functions roughly like a treaty, setting shared rules to be implemented in the national laws of Member States.⁵¹ It requires each Member State to provide special immunities for ISPs, hosts, and caching providers, and allows Member States to provide additional immunities at their discretion; legislators or courts in some countries have applied it to search engines as well.⁵² The eCommerce Directive also permits and encourages affected parties and Member States to adopt specific procedures for notice-and-takedown.⁵³ A few EU countries have used this opportunity to establish detailed protections like those listed above. For example, Finnish law requires copyright holders to provide specified information before OSPs consider a removal request, and requires OSPs to give the alleged infringers notice and an opportunity to “counter-notice” or object to removals.⁵⁴ In 2012, a European Commission study found similar laws in five other countries.⁵⁵

Many other EU countries have not legislated meaningful notice-and-takedown procedures, leaving an unfortunate degree of uncertainty about the

(discussing impact of ISP site-blocking on website operators under analogous fair trial right of European Convention on Human Rights).

50. eCommerce Directive, *supra* note 12, arts. 12–15.

51. *See Regulations, Directives, and Other Acts*, EUROPEAN UNION, <https://europa.eu/european-union/eu-law/legal-acts> [<https://perma.cc/PJF4-B5ZU>] (last visited Mar. 31, 2018).

52. *See, e.g.,* Peguera, *supra* note 5, at 542 n.178 (citing Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico [Law on Information Society and Electronic Commerce Services], art. 17 (B.O.E. 2002, 34) (Spain), <http://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf> [<https://perma.cc/9H3A-YXEH>] (providing immunity for search engines)); *see also* Société des Auteurs des Arts Visuels et de l’Image Fixe (SAIF) v. Google France, Cour d’appel [CA] [regional court of appeal] Paris, 1ère ch., Jan. 26 2011, 08/13423, <http://juriscom.net/wp-content/documents/caparis20110126.pdf> [<https://perma.cc/3T67-69ZK>] (finding safe harbors for Google’s image search under French law); *Mosley v. Google Inc.*, [2015] EWHC 59 (QB) [30] (holding that Article 13 of the eCommerce Directive “applies to internet service providers such as Google who operate a search engine”); Joris van Hoboken, *Legal Space for Innovative Ordering: On the Need to Update Selection Intermediary Liability in the EU*, 13 INT’L J. COMM. L. & POLY 1, 8–12 (2009) (detailing the position of search engines under the eCommerce Directive).

53. eCommerce Directive, *supra* note 12, recitals 40, 46.

54. Tuomas Mylly & Ulla-Maija Mylly, Council of Europe, *Finland Country Report, in* COMPARATIVE STUDY ON BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT 218, 221 n.1, 221–22 (2015), <https://rm.coe.int/1680655533> [<https://perma.cc/3VJT-KYL8>].

55. *Single Market Online Services*, *supra* note 37, at 44 (noting that procedures in Finland, Hungary, Lithuania, Spain and UK include “an obligation for intermediaries to offer a possibility to submit a counter-notice”). Even in legal systems that lack formal rules on point, the publisher’s defenses may be relevant to the “knowledge” that triggers liability for the OSP.

rights and obligations of both Internet users and OSPs.⁵⁶ Even so, the eCommerce Directive itself provides important baseline rules. First, it establishes a “knowledge” standard for OSP liability: OSPs are immune until they have “knowledge of illegal activity or information” posted by users.⁵⁷ As the CJEU has noted, mere allegations may not meet this standard if they are “insufficiently precise or inadequately substantiated.”⁵⁸ This standard makes it easier for OSPs to protect users’ rights in the face of vague or unsubstantiated removal demands. In a few cases, courts have even held that mere allegations cannot establish OSP knowledge in difficult-to-resolve cases, and that claimants must instead prove their claims to an independent authority.⁵⁹ A

56. The European Commission has now twice officially considered overhauling the notice-and-action rules for OSPs operating under the eCommerce Directive. *See* EUROPEAN COMM’N, SUMMARY OF THE RESULTS OF THE PUBLIC CONSULTATION ON THE FUTURE OF ELECTRONIC COMMERCE IN THE INTERNAL MARKET AND THE IMPLEMENTATION OF THE DIRECTIVE ON ELECTRONIC COMMERCE (2000/31/EC) (2011), http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf [<https://perma.cc/V39N-67XV>]; *Results of the Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries, Data and Cloud Computing and the Collaborative Economy*, EUROPEAN COMM’N (Jan. 26, 2016), <https://ec.europa.eu/digital-single-market/en/news/results-public-consultation-regulatory-environment-platforms-online-intermediaries-data-and/> [<http://perma.cc/2CE8-MY3D>]. Public interest groups have issued detailed critiques and suggestions for improvement. *See, e.g.*, ARTICLE 19, INTERNET INTERMEDIARIES: DILEMMA OF LIABILITY 15–19 (2013), www.article19.org/data/files/Intermediaries_ENGLISH.pdf [<https://perma.cc/2NG5-4N2D>]; *EDRi Response to European Commission E-Commerce Directive Consultation*, EUROPEAN DIG. RIGHTS 2–17 (2010), https://edri.org/files/EDRi_ecommerceresponse_101105.pdf [<https://perma.cc/754D-NZRV>]; *LQDN’s Draft Answer to the e-Commerce Consultation*, LA QUADRATURE DU NET (2010), <https://lqdn.co-ment.com/text/KALApGyXcx/view/> [<https://perma.cc/V84H-ZHNE>].

57. eCommerce Directive, *supra* note 12, art. 14(1)(a) (creating both actual and constructive knowledge standards for Internet hosts).

58. Case C-324/09, *L’Oréal SA v. eBay Int’l AG*, 2011 E.C.R. I-6011, ¶ 122.

59. *Royo v. Google* (Barcelona appellate court judgment 76/2013 of 13 February 2013) at Section 7 (on file with Berkeley Technology Law Journal); *Asociación de Internautas v. SGAE* (Spanish supreme court judgment 773/2009 of 9 December 2009), <https://bit.ly/2HANz7t> [<https://perma.cc/62S3-NU2X>] (holding that the eCommerce Directive precludes requiring court orders for every removal); *see also Davison v. Habeeb* [2011] EWHC 3031 (QB) [68] (holding that notice of an allegedly defamatory blog post did not create actual or constructive knowledge under the eCommerce Directive where OSP was “faced with conflicting claims . . . between which it was in no position to adjudicate”). Two earlier UK cases discuss the issue of OSP “knowledge” under the eCommerce Directive, noting that “in order to be able to characterise something as ‘unlawful’ a person would need to know something of the strength or weakness of available defences.” *Bunt v. Tilley* [2006] EWHC 407 (QB) [72] (Eady, J.); *Kaschke v. Gray* [2010] EWHC 690 (QB) [100] (quoting *Bunt*, [2006] EWHC 407 (QB) [72]). *But see Tamiz v. Google Inc.* [2013] EWCA Civ 68 (holding that a blogging platform can be liable as a publisher of user content under defamation law, without consideration of eCommerce hosting defenses or standard for knowledge thereunder); *see also* Alberto Aranovitz, Council of Europe, *Portugal Country Report*, in

Spanish appellate ruling provided perhaps the strongest statement of this standard, saying that OSPs should not remove such content without a court order or “set themselves up as judges of such content, since the aim is precisely to enhance freedom of expression online.”⁶⁰

A second key provision of the eCommerce Directive says that OSPs may not, under law, be given any “general obligation to monitor” or police users’ online expression.⁶¹ The ECHR and CJEU both have recognized that this rule protects fundamental rights of Internet users, in large part because monitoring requirements would foreseeably lead to over-cautious erroneous removal of lawful speech, and fewer open platforms for online participation.⁶² The ECHR

COMPARATIVE STUDY ON BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT 539, 544 (2015), <https://rm.coe.int/1680655540> [<https://perma.cc/D49Y-Y9Y2>] (explaining that under Portuguese law, OSPs are “not obliged to remove the content or to disable access to it merely because an interested party alleges that there has been a violation of the law,” but must remove only “obviously illegal” content).

60. Royo v. Google (Barcelona appellate court judgment 76/2013 of 13 February 2013) at Section 7 (author’s translation); *see also* Decision No. 2004-496 (French Constitutional Council judgment DC 2004-496 of 10 June 2004) at ¶9, <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2004/2004-496-dc/decision-n-2004-496-dc-du-10-juin-2004.901.html> [<https://perma.cc/8QPM-CPL9>] (confirming constitutionality of French eCommerce Directive implementation based in part on conclusion that hosts need remove only manifestly unlawful content or content ordered withdrawn by a court).

61. eCommerce Directive, *supra* note 12, art. 15(1). The exact parameters of the prohibited “general” monitoring obligation under EU law are disputed, and the issue is prominent in current Brussels policy discussions. *See* Daphne Keller, Comment Letter on the European Commission’s March 2018 Recommendation on Measures to Further Improve the Effectiveness of the Fight Against Illegal Content Online (Mar. 28, 2018), http://cyberlaw.stanford.edu/files/publication/files/Commission-Filing-Stanford-CIS-26-3_0.pdf [<https://perma.cc/367R-HFA9>] (discussing threats to privacy rights, information, rights, and rights against discrimination in Commission’s proposal for platforms to automatically block terrorist content); *CDT and More than 50 Human Rights Organisations Call on EU Lawmakers to Reject Upload Filters*, CTR. FOR DEMOCRACY & TECH. (Oct. 16, 2017), <https://cdt.org/press/cdt-and-more-than-50-human-rights-organisations-call-on-eu-lawmakers-to-reject-upload-filters/> [<https://perma.cc/3EX6-EXVX>] (opposing filtering mandate in proposed copyright directive); MONICA HORTEN, CTR. FOR DEMOCRACY & TECH., CONTENT ‘RESPONSIBILITY’: THE LOOMING CLOUD OF UNCERTAINTY FOR INTERNET INTERMEDIARIES 11 (2016), <https://cdt.org/files/2016/09/2016-09-02-Content-Responsibility-FN1-w-pgenbs.pdf> [<https://perma.cc/QQ7A-ZCRM>] (listing 2016 policy proposals with potential monitoring requirements for OSPs including copyright, hate speech, and countering violent extremism initiatives).

62. *See* Magyar Tartalomszolgáltatók Egyesülete (MTE) v. Hungary, App. No. 22947/13, Eur. Ct. H.R. 135 (2016), <http://hudoc.echr.coe.int/eng?i=001-167828> [<https://perma.cc/AF66-8QPN>] (holding that monitoring may not be mandated in case of defamatory speech in news forum comments); Case C-70/10, Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM), 2011 E.C.R. I-12006, 12027–28, ¶ 52 (noting that requiring an OSP to monitor user content “could potentially undermine

has rejected over-reaching monitoring obligations on fundamental rights grounds alone, leading some scholars to suggest that the prohibitions in the eCommerce Directive may be “merely an explicit confirmation . . . of a limitation that would apply anyway as a result of constitutional considerations.”⁶³

Intermediary liability law under the eCommerce Directive is far from perfect. It typically lacks detailed procedural rules, and the protections created by the “knowledge” standard and restriction of mandatory monitoring have been undercut by some courts and lawmakers.⁶⁴ But it does create basic tools to limit over-removal under notice-and-takedown systems—in striking contrast to the GDPR, as will be discussed in Section IV.B.

The eCommerce Directive applies to all or nearly all legal removal claims received by OSPs, ranging from copyright to hate speech.⁶⁵ The one potential exception is for the claims based on data protection law discussed in this

freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications”); Case C-360/10, *Belgische Vereniging van Auteurs Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, [2012] 2 C.M.L.R. 18, ¶ 50. *But see* *Delfi AS v. Estonia*, App. No. 64569/09, Eur. Ct. H.R. 586, ¶ 115 (2015), <http://hudoc.echr.coe.int/webservices/content/pdf/001-155105> [<https://perma.cc/6AVY-2YHX>] (holding that a monitoring requirement was permissible in case of unprotected hate speech in news forum comments); *see also* Daphne Keller, *New Intermediary Liability Cases from the European Court of Human Rights: What Will They Mean in the Real World?*, STAN. L. SCH. CTR. FOR INTERNET & SOC’Y (Apr. 11, 2016, 5:00 AM), <http://cyberlaw.stanford.edu/blog/2016/04/new-intermediary-liability-cases-european-court-human-rights-what-will-they-mean-real> [<https://perma.cc/5Y6V-S7H3>]. Courts and lawmakers around the world have reached similar conclusions under their own intermediary liability laws. *See, e.g.*, Corte Suprema de Justicia de la Nación [CSJN] [National Supreme Court of Justice], 28/10/2014, “Rodríguez, María Belén c. Google Inc. / daños y perjuicios,” <http://www.sajj.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-rodriguez-maria-belen-google-inc-otro-danos-perjuicios-fa14000161-2014-10-28/123456789-161-0004-1ots-eupmocsollaf> [<https://perma.cc/6876-2G3P>] (Arg.); *Singhal v. Union of India*, (2015) 12 SCC 73, ¶¶ 100, 117 (India) (holding that based on free expression considerations, a notice and takedown statute must be construed to mandate removal only based on court or other government order).

63. ANGELOPOULOS ET AL., *supra* note 21, at 28.

64. *See, e.g.*, *Tribunale di Roma [Court of Rome], Civil, TMFT Enterprises LLC- Break Media v. Reti Televisive Italiane S.p.A. (RTI)*, STAN. L. SCH. CTR. FOR INTERNET & SOC’Y (Apr. 27, 2016), <http://wilmap.law.stanford.edu/entries/tribunale-di-roma-court-rome-civil-tmft-enterprises-llc-break-media-v-reti-televisive> [<https://perma.cc/CLB4-ZBP5>] (noting that the Court of Rome determined that an ad-supported video host was ineligible for immunity); HORTEN, *supra* note 61, at 11–18 (discussing legislative threats to the eCommerce Directive).

65. *See* Opinion of Advocate General Szpunar, Case C-484/14, *McFadden v. Sony Music Entm’t Ger. GmbH*, 2016 E.C.R. 170, ¶ 64 (noting that immunity extends to “all forms of liability for unlawful acts of any kind, and thus to liability under criminal law, administrative law and civil law”).

Article.⁶⁶ This had little significance before the rise of the RTBF, because data protection law was not widely used as a ground for removing online content. Now, however, excluding these claims from the eCommerce Directive notice-and-takedown framework may have real consequences—depriving Internet users of procedural protections against over-removal.

B. DATA PROTECTION HISTORY AND LAW

The law of data protection is generally very foreign to U.S. lawyers, but better known in much of the world.⁶⁷ Versions of it exist in over a hundred countries,⁶⁸ often modeled on Europe's 1995 Data Protection Directive (1995 Directive).⁶⁹

In the EU, data protection is a fundamental right, distinct from the right to privacy.⁷⁰ It emerged from twentieth-century concerns regarding large-scale records and databases tracking information about citizens, and serves to protect an individual's sphere of "informational autonomy" against such activity.⁷¹ Data protection claims can extend to any information relating to oneself, not just information that is intimate, embarrassing, or offensive. It provides legal rights against acts, like an employer's ongoing storage of outdated employee files, for which courts might not recognize a privacy claim. When the right to data protection conflicts with other fundamental rights—including rights to receive and impart information—lawmakers must balance the rights.⁷²

66. See *infra* Section II.C.

67. See generally Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877 (2014) (comparing U.S. and European laws and conceptions of privacy); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004) (comparing philosophical bases of U.S. and European privacy laws).

68. Graham Greenleaf, *Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority*, 133 PRIVACY L. & BUS. INT'L REP. 14 (2015) (listing 109 countries).

69. Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (EC) [hereinafter 1995 Directive]; see generally Schwartz & Solove, *supra* note 67 (comparing U.S. and European approaches); Whitman, *supra* note 67 (same).

70. See Charter, *supra* note 44, arts. 7, 8.

71. See, e.g., Cécile de Terwangne, *The Right to be Forgotten and Informational Autonomy in the Digital Environment*, in THE ETHICS OF MEMORY IN A DIGITAL AGE 82, 82 (Alessia Ghezzi et al. eds., 2014); Viktor Mayer-Schönberger & Yann Padova, *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation*, 17 COLUM. SCI. & TECH. L. REV. 315, 318–20, 332 (2016); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 562 (1995).

72. See, e.g., Case C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 2008 E.C.R. I-00271, 346–47, ¶ 70; Case C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*, 2014 EUR-Lex CELEX LEXIS

European data protection law establishes a detailed regulatory system, enforced by national and subnational Data Protection Authorities (DPAs).⁷³ DPAs review claims about violations of data protection law.⁷⁴ In some cases, they conduct audits and investigations.⁷⁵ The 1995 Directive required entities operating as data “controllers” to file detailed notifications with these regulators before processing data.⁷⁶

Data protection law governs the “processing” of “personal data.” Both terms are defined very broadly. Personal data includes “any information relating to an identified or identifiable natural person”⁷⁷ “Processing” is:

[A]ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.⁷⁸

These definitions bring a remarkable array of activities and information within the ambit of data protection law—from online restaurant orders to historical archives to privately operated websites.⁷⁹

Entities may process personal data only if they meet one of the six justifications enumerated under law—for example, if they have the consent of the data subject or are legally obliged to process the data.⁸⁰ A catch-all category

62012CJ0314 ¶ 63 (Mar. 27, 2014) (recognizing “the requirement that a fair balance be found . . . between all applicable fundamental rights” when implementing injunctions).

73. 1995 Directive, *supra* note 69, art. 28 (establishing supervisory authorities).

74. GDPR, *supra* note 6, art. 4(1); 1995 Directive, *supra* note 69, art. 28(4) (using identical language).

75. Olivier Proust, *Are DPA Notifications Obsolete?*, INT’L ASS’N PRIVACY PROFS. (Oct. 24, 2014), <https://iapp.org/news/a/are-dpa-notifications-obsolete/> [<https://perma.cc/MFZ7-VBWK>].

76. 1995 Directive, *supra* note 69, art. 18 (creating an obligation to notify supervisory authorities).

77. *Id.* art. 2(a).

78. GDPR, *supra* note 6, art. 4(2); 1995 Directive, *supra* note 69, art. 2(b) (using nearly identical language).

79. Case C-101/01, *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, 2003 E.C.R. I-12976, 13008–09 ¶ 27, 13021 (holding that a defendant violated the 1995 Directive by operating a website for her church listing volunteers’ names, telephone numbers, hobbies, and in one case “sensitive” medical information about a recent injury).

80. GDPR, *supra* note 6, art. 6; 1995 Directive, *supra* note 69, arts. 7, 9, 13. The GDPR and 1995 Directives effectively authorize some other uses of data that are not listed in these sections through other exemptions or derogations, such as those covering journalism. *See infra* Section III.D.

permits processing “necessary for . . . legitimate interests”⁸¹ As will be discussed below, this “legitimate interests” criterion is key for OSP operations under both the 1995 Directive and the GDPR.⁸²

For entities subject to data protection law, a key distinction is whether the law classifies them as “controllers” or “processors.” Distinct legal obligations flow from each classification. Controllers are, roughly speaking, entities that hold personal data and decide what to do with it.⁸³ Because they are the decisionmakers, they have far more obligations under the law. Importantly for this Article, this includes compliance with erasure or RTBF requirements.

On the other hand, processors hold personal data, but follow instructions from a controller about what to do with it.⁸⁴ Their legal duties are correspondingly fewer—they include maintaining data security and abiding by the controller’s contractual requirements.⁸⁵ In a simple example, a firm that holds records about its employees is a controller of their personal information; if it outsources payroll operations by instructing a payroll company, that company is a processor.

The person whose personal data is being processed is called the “data subject.” A data subject’s rights include access, rectification, and erasure of data held by controllers.⁸⁶

This framework emerged from an era when data processing was largely a matter for banks, employers, sports clubs, doctors, and other brick-and-mortar entities.⁸⁷ Because it was designed with databases in mind, it provides a good framework for some things that Internet companies do, such as tracking, collecting, and storing data about user behavior.⁸⁸ As will be discussed below,

81. GDPR, *supra* note 6, art 6(f); 1995 Directive, *supra* note 69, art. 7(f) (using identical “necessary for . . . legitimate interests” language).

82. *See infra* Section II.C.

83. *See* 1995 Directive, *supra* note 69, art. 2(d) (“‘Controller’ shall mean the natural or legal person . . . which alone or jointly with others determines the purposes and means of the processing of personal data”); GDPR, *supra* note 6, art. 4(7) (similar language).

84. *See* 1995 Directive, *supra* note 69, art. 2(e) (“‘Processor’ shall mean a natural or legal person . . . which processes personal data on behalf of the controller”); GDPR, *supra* note 6, art. 4(8) (similar language); *see also* ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 1/2010 ON THE CONCEPTS OF “CONTROLLER” AND “PROCESSOR” 25 (2010), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf [<https://perma.cc/4CMK-7WTR>].

85. *See* 1995 Directive, *supra* note 69, art. 17 (requiring controllers to contractually impose security requirements on processors); ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 84, at 25.

86. GDPR, *supra* note 6, arts. 15–17; 1995 Directive, *supra* note 69, art. 12.

87. *See generally* GLORIA GONZALEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 111–23 (2014) (discussing antecedents to 1995 Directive in laws addressing 1970s commercial data processing operations).

88. *See id.*

though, expansion of platforms that support online user expression created significant difficulties in mapping the data protection framework onto unanticipated technologies.

C. DATA PROTECTION AND ONLINE SERVICE PROVIDERS

OSPs are complex creatures under data protection law. In one respect, as operators of proprietary back-end databases and storage systems containing records of users' clicks, purchases, and other online behavior, they look like classic data controllers. At the same time, OSPs process content created and shared by their users—and sometimes that content includes data about other people. A user who posts a photo or a comment about another person is putting *that* data subject's personal data in the hands of an OSP. Identifying the OSP's duties to both the speaker and the person being spoken about and fitting online speech into a traditional data protection legal framework is difficult.

Suppose someone tweets, "Matilda Humperdink served bad fish at her party last night. We all got sick—even Matilda!" That person is acting as a controller of data about Matilda including the "sensitive" data about her health, which typically may not be processed without her consent.⁸⁹ Does Twitter become a controller of that information as well? Can Matilda oblige Twitter to delete the post?⁹⁰ If Google indexes the tweet, what obligations does it have? Should the answers to these questions change if Matilda is the CEO of a fast-food restaurant chain with a poor sanitation record, and the party was one of her restaurant openings? Because data protection law has historically applied to back-end processing, such as stored hospital records or Internet

89. GDPR, *supra* note 6, art. 9; 1995 Directive, *supra* note 69, art. 8; ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 5/2009 ON ONLINE SOCIAL NETWORKING 8 (2009), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf [<https://perma.cc/36TA-2SPY>].

90. The removal question is simpler when fewer parties are involved. A data subject would generally be entitled to remove his or her own tweet. And if Matilda asked the original author to delete the tweet, instead of asking Twitter, the author would have to assess her own duties as controller (potentially jointly with Twitter) of the data in the tweet. *See generally* Brendan van Alsenoy, *The Evolving Role of the Individual Under EU Data Protection Law* 22–23 (KU Leuven Ctr. for IT & IP Law, CiTiP Working Paper 23/2015, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641680 [<https://perma.cc/D3Y6-9BYH>]. The CJEU will address important questions about social media users' duties in a pending case against an individual who posted footage of on-duty police officers to YouTube. *See* Case C-345/17, *Sergejs Buivids v. Datu Valsts Inspekcija*, 2017 EUR-Lex CELEX LEXIS 62017CN0345 (June 12, 2017), <http://eur-lex.europa.eu/legal-content/EN/TEXT/PDF/?uri=CELEX:62017CN0345> [<https://perma.cc/6U5L-CEJX>].

user logs, it has rarely needed the doctrinal tools to answer questions like these about public information and speech.⁹¹

The expression posted by users on OSP platforms is a form of data, but it is very different from the back-end files, logs, or profiles typically governed by data protection law. The difference between public expression and back-end data is very important because the two types of data differ not only as a technical matter, but as a matter of fundamental rights.

When an Internet company generates back-end data by tracking user activity, only two sets of rights are generally affected: those of the user and those of the company. Giving the user a simple, streamlined way to enforce data protection rights against the company makes sense procedurally, since there is no reason to involve any third parties. And it makes sense for the rules to favor erasure, because users' rights to delete back-end data are relatively straightforward.

For public expression, like the tweet about Matilda Humperdink, the situation is very different. A request to erase this data affects at least four sets of rights: the author's rights to free expression, Matilda's rights to data protection and privacy, other Internet users' rights to seek and access information, and Twitter's rights as a business.⁹² Rules that make sense for the simpler two-party situation of back-end data erasure will not work well to protect all of these conflicting interests. Adding expression and information rights to the mix makes barriers to improper data erasure much more important.

Data protection experts recognized and wrestled with these issues as Internet platforms matured in the late 2000s. The Article 29 Working Party, a regulatory organization established under the 1995 Directive,⁹³ issued highly influential, though nonbinding, opinions about both social media⁹⁴ and search

91. Many possible tensions between data protection and free expression are alleviated by exceptions in the law for journalism, resulting in a body of law tailored to that context; it is generally less helpful for ordinary Internet users. See David Erdos, *Beyond 'Having a Domestic'? Regulatory Interpretation of European Data Protection Law and Individual Publication*, 33 *COMPUTER L. & SECURITY REV.* 275, 277–78 (2017).

92. Twitter's own expression and information rights, and other rights discussed *infra* Section III.A, may also be implicated.

93. 1995 Directive, *supra* note 69, art. 29(1) (creating the Article 29 Working Party and noting that it has "advisory status"); see also *Opinions and Recommendations*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm [<https://perma.cc/7AZP-RVMA>] (last visited Apr. 1, 2018).

94. See ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 89; ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 84. In the more recent opinion, the Working Party suggested that social networks and their users are both controllers with respect to information posted by the user, while a telecommunications operator offering bare-bones email services is

engines in this period.⁹⁵ The opinions, which do not address real cases but instead provide general guidance to DPAs and regulated entities, included both legal analysis and hypothetical examples. These opinions were to some extent superseded by subsequent developments—including *Google Spain* and the GDPR—but they remain good windows into the difficulty of fitting OSPs into the data protection framework. Rules designed for databases and back-end data processing are hard to apply to OSPs processing Internet users' communications.

The Article 29 Working Party opined that social media platforms are data controllers.⁹⁶ The opinion did not probe the differences between back-end data and user-generated expression, but its discussion indicated that expression was considered data and thus subject to data protection law. For example, it said that if a user uploads a photo of another person that reveals "sensitive" information about the person's health, the OSP must obtain explicit consent from *that* person before processing the picture.⁹⁷ If correct, this classification leads to strange results. For example, if Twitter has the legal obligations of a controller, then it breached data protection law the moment its user tweeted about Matilda Humperdink's illness.⁹⁸ As another example, the Article 29 social media opinion suggests that platforms must let people access, correct, or delete information posted about them—without accounting for the privacy expectations of authors who post remarks about other people in private messages or closed groups.⁹⁹

to "be considered controller only for traffic and billing data, and not for any data being transmitted" in the email. *See* ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 84, at 11, 21.

95. ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 1/2008 ON DATA PROTECTION ISSUES RELATED TO SEARCH ENGINES 23 (2008), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf [<https://perma.cc/7JWJ-8CVG>].

96. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 89, at 5.

97. *See id.* at 7–8; *infra* Section III.B (discussing the scant case law to date); Natali Helberger & Joris van Hoboken, *Little Brother is Tagging You—Legal and Policy Implications of Amateur Data Controllers*, 4 COMPUTER L. REV. INT'L 101, 104.0 (2010); Erdos, *supra* note 91, at 277–78; Van Alsenoy, *supra* note 90, at 10–12.

98. Following the Working Party's analysis, Twitter would require consent unless Matilda had already published the data. *See* ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 89, at 8. They could not seek her consent, however, unless she were already a platform member, because "a possible e-mail invitation to join the SNS in order to access these personal data would violate the prohibition laid down in Article 13.4 of the ePrivacy Directive . . ." *Id.*

99. *Id.* at 11. The Working Group's opinion would also prohibit social networks from retaining information about the reasons a user's account was terminated, and allow them to retain information identifying those accounts for only a year. *Id.* at 10. This is difficult to reconcile with other standard operations of OSP hosts, including the repeat infringer policies of the U.S. DMCA. *See* 17 U.S.C. § 512 (2012).

In contrast, the search engine opinion is more thoughtful regarding the distinction between back-end “user data” and what it calls “content data”—expression and information from third party webmasters, which Google indexes.¹⁰⁰ For “content data,” the opinion says that search engine providers are generally not to be held primarily responsible under European data protection law.¹⁰¹ Thus, a search engine “should not be considered to be the principal controller with regard to the content The formal, legal and practical control the search engine has over the personal data involved is usually limited to the possibility of removing data from its servers.”¹⁰²

This distinction, though helpful, still does not fully reconcile the operations of search engines or other OSPs with EU data protection requirements. For one thing, OSPs’ legal justification for processing “content data” in the first place is the catch-all provision for “legitimate interests.”¹⁰³ This vague “legitimate interests” concept is a slim reed upon which to rest the entire edifice of OSP operations. As discussed above, it is also legally insufficient for processing health status and other sensitive personal data.¹⁰⁴ As a result, as Professor Miquel Peguera has noted, classifying search engines as controllers would seemingly render them “incompatible with EU law” because they are “unable to comply with most of the obligations the Directive imposes on data controllers.”¹⁰⁵ These longstanding questions about OSPs and data protection law may finally be resolved soon, however. As this Article went to press, the CJEU was considering a new case brought by data subjects who opposed both Google’s and the French DPA’s failure to grant their RTBF requests. That

100. See ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 95, at 24.

101. *Id.*

102. *Id.* at 14.

103. GDPR, *supra* note 6, art. 6.1(f); 1995 Directive, *supra* note 69, art. 7(f); see also ARTICLE 29 DATA PROT. WORKING PARTY, GUIDELINES ON THE IMPLEMENTATION OF THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT ON “GOOGLE SPAIN AND INC. V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLES” C-131/12 at 5 (2014), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf [<https://perma.cc/6LPR-TFRL>] (“The legal ground for [search engine] processing under the EU Directive is to be found in Article 7(f)”).

104. GDPR, *supra* note 6, art. 9; 1995 Directive, *supra* note 69, art. 8(2) (listing legal bases for processing sensitive data).

105. Peguera, *supra* note 5, at 539. As another example, controllers generally must notify data subjects at the time of collecting data about them from third parties. 1995 Directive, *supra* note 69, art. 11. For OSPs that “collect” users’ posts, identifying and notifying any individual mentioned would be more than difficult. For this requirement, OSPs can invoke an exemption based on difficulty, but it is noteworthy that the central data protection concept of notice is so ill-suited to OSPs processing user-generated content.

case squarely raises questions about search engines' legal grounds for processing sensitive personal data.¹⁰⁶

D. THE *GOOGLE SPAIN* RULING

Mounting concerns about online data protection came to a head in the CJEU's *Google Spain* case. The case is explained in detail in numerous other sources, so this Article will summarize it only briefly.¹⁰⁷

The case concerned a Spanish man, Mario Costeja González, whose property was auctioned for nonpayment of debts in 1998.¹⁰⁸ A Barcelona newspaper, *La Vanguardia*, published a legally mandated announcement of the auction, including Mr. Costeja's name.¹⁰⁹ Ten years later, the paper digitized its archives and made them available online.¹¹⁰ People using Google to search for Mr. Costeja's name could find the notice among the top results.¹¹¹ Mr. Costeja, who had since resolved his financial problems, complained to the Spanish DPA and obtained an order for Google to remove the results.¹¹²

Google appealed the order through the Spanish courts, which eventually referred key questions to the CJEU. Answers to the doctrinal questions raised in the case were far from clear.¹¹³ The CJEU's own Advocate General—whose advice the court typically follows—said the DPA's removal order was not valid.¹¹⁴

106. Press Release, Conseil d'État, Right to Be Delisted (Feb. 24, 2017) <http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted> [<https://perma.cc/5UT2-HUWS>].

107. See, e.g., Peguera, *supra* note 5, at 522–34; see also generally van Hoboken, *supra* note 5.

108. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317, ¶ 14.

109. Peguera, *supra* note 5, at 523.

110. *Id.*

111. *Id.*

112. *Id.* at 523–24.

113. These included detailed questions about jurisdiction and the applicability of the 1995 Directive to Google's American parent company, Google Inc.; questions about data processing and whether Google acted as a controller for indexed data; and questions about the existence and scope of the RTBF under Articles 12 and 14. See *Google Spain*, 2014 E.C.R. 317, ¶ 20.

114. The Advocate General, who functions somewhat like a prestigious, public clerk in recommending outcomes to the court, concluded that Google in most cases does not act as a controller. Opinion of Advocate General Jääskinen, Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2013 E.C.R. 424, ¶ 89. In any case, Advocate General Jääskinen concluded that the 1995 Directive did not create a right to “be forgotten” by deleting publicly available information based on the data subject's personal preference. *Id.* ¶ 111. See also generally Carlos Arrebola et al., *An Econometric Analysis of the Influence of the Advocate General on the Court of Justice of the European Union*, 5 CAMBRIDGE J. INT'L & COMP. L. 82, 84, 106

The court, however, found in Mr. Costeja's favor. Critically, it concluded that Google acted as the controller of the indexed auction announcement, because it determined the purposes and means by which it processed that content.¹¹⁵ The court focused on Google's indexing function, noting that web search engines aggregate disparate, previously unconnected information "to establish a more or less detailed profile of the data subject" in the form of search results.¹¹⁶ This processing, the court noted, was different than the processing involved in *La Vanguardia's* posting of the auction notice, and was subject to separate analysis and obligations under data protection law.¹¹⁷ For this reason, a search engine could be obliged to remove links to information on webpages even "when its publication in itself on those pages is lawful."¹¹⁸

The court said that as a controller, Google must honor erasure requests and objections to processing under the 1995 Directive.¹¹⁹ It established what was effectively a notice-and-takedown process, without reference to Google's status as a protected intermediary under Spain's implementation of the eCommerce Directive.¹²⁰ Specifically, Google must remove the specified links from the list of results that appear when users search for the data subject's name.¹²¹ However, the same results could still appear in results for other search terms. For example, a page discussing Matilda Humperdink's food poisoning might still appear when people search for "fish," but not when they search for "Matilda Humperdink." In practice this meant that data from the page, usually including all its text, would also persist on Google's servers to power its search results.

(2016) (finding that the Advocate General's opinion has a statistically significant effect on the Court of Justice's decision outcomes).

115. *See Google Spain*, 2014 E.C.R. 317, ¶ 1 (applying the definition of controller from Article 2(d) of the 1995 Directive, *supra* note 69).

116. *Id.* ¶ 37.

117. *Id.* ¶¶ 82, 85–88.

118. *Id.* ¶ 88.

119. *Id.* ¶ 3 (citing 1995 Directive, *supra* note 69, arts. 12, 14). The court did not clearly distinguish how the two separate rights it cited—the Article 12 right to "rectification, erasure or blocking" or the Article 14 right to "object" to processing—shaped its decision. In a subsequent ruling rejecting a RTBF claim against a government-mandated corporate registry, however, the court elaborated some relevant doctrinal differences between the two articles. Case C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017 EUR-Lex CELEX LEXIS 62015CJ0398 ¶¶ 56–60 (Mar. 9, 2017).

120. *Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico* [Law on Information Society and Electronic Commerce Services], arts. 14–17 (B.O.E. 2002, 34) (Spain).

121. *Google Spain*, 2014 E.C.R. 317, ¶ 82.

The court was less clear about how Google, or other search engines, should determine which removal requests to honor.¹²² It instructed them to remove data that is inaccurate or “inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing,”¹²³ even if the information is true¹²⁴ or causes no prejudice to the data subject.¹²⁵

RTBF requests are not to be honored, though when “the interference with [the requester’s] fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.”¹²⁶ However, “as a rule,” the public’s general interest in information does not outweigh the data subject’s data protection interests.¹²⁷ The court did not identify or discuss the free expression rights of the website operator or publisher, or how exclusion from some Google search results could affect those rights.¹²⁸ This prioritization of data protection over other rights generated considerable controversy both in popular press and among legal experts.¹²⁹

122. Some object to the term “removal” to describe the delisting required by *Google Spain*, because the data still appears in other search results. See, e.g., Joe McNamee, *Google’s Forgetful Approach to the “Right to Be Forgotten”*, EUR. DIGITAL RTS. (Dec. 14, 2016), <https://edri.org/googles-forgetful-approach-right-forgotten/> [<https://perma.cc/D4GQ-ZZQ4>]. This Article uses “removal” to refer both to search indexes delisting information and hosts deleting it. This broad sense of the word, encompassing both complete and partial deletion, has long been conventional in the intermediary liability context. See, e.g., John Mueller, *URL Removals Explained, Part II: Removing Sensitive Text from a Page*, GOOGLE (Aug. 6, 2010), <https://webmasters.googleblog.com/2010/04/url-removals-explained-part-ii-removing.html> [<https://perma.cc/3GCC-LSFT>] (describing process to “remove the snippet and the cached page” while leaving the rest of a search result intact); Lorenzo Franceschi-Bicchierai, *The Countries Where Facebook Censors the Most Content*, MASHABLE (Nov. 7, 2014), <http://mashable.com/2014/11/07/facebook-censorship-map/> [<https://perma.cc/5X7R-GRNE>] (describing content as “removed” when Facebook blocks some but not all users from seeing it based on national law).

123. *Google Spain*, 2014 E.C.R. 317, ¶¶ 92, 94 (paraphrasing 1995 Directive, *supra* note 69, art. 6.1(c)).

124. *Id.* ¶ 94.

125. *Id.* ¶ 96.

126. *Id.* ¶ 97.

127. *Id.* (“[I]hose rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject’s name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified . . .”).

128. See Peguera, *supra* note 5, at 555. The newspaper that published Mr. Costeja’s information was not a party to the CJEU case, so no one before the court directly represented publishers’ interests. See *id.*

129. See, e.g., van Hoboken, *supra* note 5, at 2 (observing that the CJEU’s requirement of “effective and complete” protection for data protection rights is in tension with the broader need to balance data protection against other fundamental rights). Other important critiques

In nearly four years following the ruling, Google and Microsoft's Bing were asked to delist nearly over 2.6 million URLs, and actually delisted approximately one million.¹³⁰ Norms and standards, including thoughtful guidelines from the Article 29 Working Party, have begun to emerge to guide search engines in distinguishing valid from invalid RTBF requests.¹³¹ Some cases in which Google declined to delist have been brought to DPAs and national courts, creating a small but growing body of precedent.¹³²

When Google *does* remove results, however, there is almost no analogous public review. Publishers do not have recourse to a regulatory agency to review their free expression claims, and may lack legal standing to challenge a removal in any case.¹³³ Thus, courts and regulators have ample opportunity to enforce the status quo or to require more delisting, but there is no good mechanism for them to move the needle in the other direction—toward delisting less.

While some degree of consensus has emerged on the substantive criteria for RTBF removals, the same cannot be said for the procedure and technical implementation.¹³⁴ In particular, disputes about jurisdiction have grown increasingly acute. In 2017, the CJEU agreed to review a case arising from the French DPA's order that Google remove search results globally, even in countries that do not recognize a RTBF.¹³⁵

of the ruling, including many rooted in intermediary liability concerns, are well summarized in Kuczerawy & Ausloos, *supra* note 5.

130. *Search Removals Under European Privacy Law*, GOOGLE, <https://www.google.com/transparencereport/removals/europeprivacy/> [<https://perma.cc/KA44-UBMQ>] (last visited Mar. 31, 2018) (reporting 56.2% of URL removal requests rejected); MICROSOFT, *supra* note 9 (reporting 46% of URL delist requests accepted); BERTRAM ET AL., *supra* note 8 (providing detailed quantitative breakdown of requests).

131. *See, e.g.*, ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103; *see also* LUCIANO FLORIDI ET AL., THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN 7–14 (2015), <https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf> [<https://perma.cc/885T-6436>].

132. *See* Stefan Kulk & Frederik Borgesius, *Freedom of Expression and 'Right to Be Forgotten' Cases in the Netherlands After Google Spain*, 1 EUR. DATA PROTECTION L. REV. 113, 117–23 (2015); Miquel Peguera, *No More Right-to-Be-Forgotten for Mr. Costeja, Says Spanish Data Protection Authority*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y (Oct. 3, 2015, 8:24 AM), <http://cyberlaw.stanford.edu/blog/2015/10/no-more-right-be-forgotten-mr-costeja-says-spanish-data-protection-authority> [<https://perma.cc/TK2Q-SBMZ>] (describing how Spain's DPA rejected Mr. Costeja's removal requests following the CJEU ruling).

133. *See infra* Section III.D.2.

134. *See* ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103; *see also* FLORIDI ET AL., *supra* note 131, at 15–21.

135. Press Release, Conseil D'État, CE, July 19, 2017, GOOGLE INC. (July 19, 2017), <http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC> [<https://perma.cc/P93U-5Y72>]. The French DPA published an unofficial English translation

DPAAs have also clashed with Google on questions about transparency for RTBF removals. The Article 29 Working Party disputed Google's practice of routinely notifying webmasters when pages from their sites were removed from search results, arguing that the company should notify and consult with webmasters only in exceptional, difficult cases.¹³⁶ And in 2017, the Spanish DPA fined Google €150,000 for telling a webmaster about a RTBF removal.¹³⁷ Some public debate has centered on Google's attempts to notify users when search results were modified in response to RTBF requests.¹³⁸ Outside the context of search indexes, some national courts have ordered information erased or delisted from websites, including those of newspapers, based on RTBF claims.¹³⁹

of its decision, explaining its reasoning. Commission Nationale de l'Informatique et des Libertés [CNIL] [National Commission on Informatics and Liberty], Mar. 10, 2016, 2016-054, <http://sites.les.univ.fr/cybercrime/wp-content/uploads/2017/08/2016-google.pdf> [<https://perma.cc/9BC4-ZR53>].

136. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 10; AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, RESOLUCIÓN: R/02232/2016 at 50 (2016), www.agpd.es/portaleswebAGPD/resoluciones/procedimientos_sancionadores/ps_2016/comun/pdfs/PS-00149-2016_Resolucion-de-fecha-14-09-2016_Art-ii-culo-10-16-LOPD.pdf [<https://perma.cc/JZK9-R5CV>].

137. See David Erdos, *Communicating Responsibilities: The Spanish DPA Targets Google's Notification Practices when Delisting Personal Information*, INFORM'S BLOG (Mar. 21, 2017), <https://inform.wordpress.com/2017/03/21/communicating-responsibilities-the-spanish-dpa-targets-googles-notification-practices-when-delisting-personal-information-david-erdos/> [<https://perma.cc/G5Q3-3XX4>].

138. Notice about removals to people seeking content online is another important check on over-removal. Google tried to address this for the RTBF through near-ubiquitous notices on search results pages. See Danny Sullivan, *How Google's New "Right to Be Forgotten" Form Works: An Explainer*, SEARCH ENGINE LAND (May 30, 2014, 2:54 AM), <https://searchengineland.com/google-right-to-be-forgotten-form-192837> [<https://perma.cc/VEC8-MH6Q>]. These do not specify what content was removed, though, and the Article 29 Working Party has said Google would violate the law if they did. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 3.

139. See, e.g., P.H. v. O.G., Cour de Cassation [Cass.] [Court of Cassation] Belgique, Apr. 29, 2016, N° C.15.0052.F (Belg.), http://jre.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20160429-1 [<https://perma.cc/J53D-BLM5>] (ordering news archive to anonymize story); see also Hugh Tomlinson, *Case Law, Belgium: Olivier G v. Le Soir. "Right to be Forgotten" Requires Anonymisation of Online Newspaper Archive*, INFORM'S BLOG (July 19, 2016) <https://inform.org/2016/07/19/case-law-belgium-olivier-g-v-le-soir-right-to-be-forgotten-requires-anonymisation-of-online-newspaper-archive-hugh-tomlinson-qc> [<https://perma.cc/7D4D-VV9V>]; Athalie Matthews, *How Italian Courts Used the Right to Be Forgotten to Put an Expiry Date on News*, GUARDIAN (Sept. 20, 2016, 4:12 AM), <https://www.theguardian.com/media/2016/sep/20/how-italian-courts-used-the-right-to-be-forgotten-to-put-an-expiry-date-on-news> [<https://perma.cc/VG27-CGVL>] (noting that lower Italian court fined the newspaper €5,000 and confiscated the editor's car as security); NICOLAS KAYSER-BRIL & MARIO TEDESCHINI-LALLI, OFFSHORE JOURNALISM: PRELIMINARY REPORT (2017), <http://www.offshorejournalism.com/data/Offshore%20Journalism%20Report.pdf>

Oceans of scholarly ink have been spilled discussing the *Google Spain* case and the questions it generated. But to date, there has been almost no public discussion of the RTBF under the legislation that has now taken its place: the EU's sweeping new GDPR.

E. THE 2016 GENERAL DATA PROTECTION REGULATION

The GDPR is a comprehensive overhaul of EU data protection law, codifying new rules for the RTBF and much more.¹⁴⁰ As will be discussed throughout this Article, it introduces new rules that are both harder to understand than those established by *Google Spain* and more dangerous to online information and expression.

The new Regulation is much more expansive than its precursor, replacing the 1995 Directive's scant 12,000 words with over 50,000 new ones, developed through multiple drafts and years of discussion.¹⁴¹ Because it is a Regulation rather than a Directive, it does not have to be implemented as separate legislation in each EU country.¹⁴² It went into effect across the EU automatically in May of 2018.¹⁴³

The GDPR makes sweeping changes to data protection law. For OSPs, many of the law's most important new terms are not about users' expression, but rather about the companies' own collection and use of back-end stored data about user behavior. Complying with those new rules may require engineering work to change logging and storage,¹⁴⁴ user interface redesign to introduce new notices and consent processes,¹⁴⁵ written Data Protection

[<https://perma.cc/4UHA-PPE7>] (describing news editors' and reporters' experiences with RTBF requests).

140. See W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAW. 221, 225–26 (2017).

141. See, e.g., *The History of General Data Protection Regulation*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [<https://perma.cc/W6D3-FZXU>] (last visited Nov. 3, 2017); *Opinions & Papers*, WILSON SONSINI GOODRICH & ROSATI, LLP, <https://www.wsgr.com/eudataregulation/opinions-papers.htm> [<https://perma.cc/9YLQ-8DZJ>] (last visited Mar. 31, 2018) (documenting guidelines, opinions, DPA papers, and stakeholder position papers).

142. See EUROPEAN UNION, *supra* note 51.

143. GDPR, *supra* note 6, art. 91(2); EUROPEAN COMM'N, *supra* note 6.

144. GDPR, *supra* note 6, arts. 5 (“Principles relating to processing of personal data”), 25 (“Data protection by design and by default”).

145. *Id.* arts. 12–13 (identifying new categories of information that must be included in privacy policies or similar notices); *id.* arts. 6(1)(a), 7, 9(1), 9(2)(a) (identifying conditions for consent to processing); HUNTON & WILLIAMS, *THE PROPOSED EU GENERAL DATA PROTECTION REGULATION: A GUIDE FOR IN-HOUSE LAWYERS* 23, 28 (2015), https://www.hunton.com/images/content/3/0/v2/3094/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf [<https://perma.cc/9NLE-CTN6>].

Impact Assessments,¹⁴⁶ extensive new internal recordkeeping,¹⁴⁷ contract renegotiation with other controllers or processors,¹⁴⁸ and in many cases the appointment of a data protection officer residing in the EU.¹⁴⁹ One influential industry group estimates that the GDPR will create 75,000 data protection officer positions.¹⁵⁰ A guide for in-house lawyers concludes that, under the GDPR, “[d]ata protection will be as significant as antitrust in terms of compliance risk,” and is “likely to require organisation-wide changes for many businesses.”¹⁵¹ One set of researchers—funded by Google—predicted that small and medium enterprises would need to increase IT budgets by sixteen to forty percent to comply with the GDPR.¹⁵²

The GDPR also stakes out expansive new extraterritorial application to companies outside of the EU,¹⁵³ and arms regulators with the power to impose unprecedented fines: in principle, these could be as high as four percent of a company’s annual global turnover or twenty million euros.¹⁵⁴ The GDPR also establishes a new European Data Protection Board, a successor organization to the Article 29 Working Party with broader powers and responsibilities.¹⁵⁵

Significant questions remain about what the new law actually means. As discussed in Section III.C, it introduces ambiguous new language in some cases and in others reuses formulations from the 1995 Directive that have long been subject to disputed interpretations. This leaves considerable room for interpretation by regulators and courts.

Two sets of authorities will be particularly well positioned to proactively resolve questions about the RTBF and information rights under the GDPR. The first is the European Data Protection Board, which is charged with issuing best practices guidelines for RTBF procedures.¹⁵⁶ The second is EU Member

146. GDPR, *supra* note 6, art. 35.

147. *Id.* art. 30.

148. *Id.* arts. 28–30.

149. *Id.* arts. 37–39.

150. INT’L ASS’N OF PRIVACY PROF’LS, THE GDPR DEMANDS 75K DPOs: WHERE WILL THEY COME FROM?, <https://iapp.org/media/pdf/DPA-Whitepaper.pdf> [<https://perma.cc/3AWM-YCHN>] (last visited Mar. 31, 2018).

151. HUNTON & WILLIAMS, *supra* note 145, at 6.

152. L. Christensen et al., The Impact of the Data Protection Regulation in the E.U. (Feb. 13, 2013) (unpublished manuscript), http://www.analysisgroup.com/uploadedfiles/content/insights/publishing/2013_data_protection_reg_in_eu_christensen_rafert_etal.pdf [<https://perma.cc/39U3-7CNC>].

153. *See infra* Section III.E.

154. GDPR, *supra* note 6, art. 83(5).

155. *Id.* art. 68 (establishing the European Data Protection Board), 94(2) (explaining that references to Article 29 of the 1995 Directive in existing law should be construed as references to Board going forward).

156. *Id.* art. 70(1)(d).

State legislatures, which are charged with protecting free expression under the GDPR, and which have surprisingly broad additional powers to modify the Regulation's terms in their national law.¹⁵⁷ Litigation and court rulings, too, will eventually shape understanding of the GDPR. But litigation is not a good avenue for mitigating risks posed by the GDPR, both because it would address issues only in piecemeal fashion and because of the practical situation of potential litigants: online publishers and speakers will have little opportunity to contest improper removal of their expression, and OSPs may be reluctant to do so on their behalf. Action by regulators is therefore particularly important.

III. THREATS TO INTERNET USERS' RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION

This Part reviews the GDPR's rules governing RTBF requests in detail, and identifies ways in which they tilt the playing field against the person whose online expression is affected. This imbalance affects both expression and privacy rights of online speakers, as well as the information rights of their readers—often in ways the drafters surely did not intend. An underlying problem with these GDPR provisions is their opacity. As Section III.A discusses, if OSPs do not understand what the law requires, the safe course will be to simply remove or delist information.

Section III.B considers whether RTBF requirements will apply to Internet hosts like Twitter or DailyMotion—a highly consequential question on which the GDPR is silent. Next, Section III.C walks through an OSP's process for notice-and-takedown under the GDPR—a process that will shape substantive outcomes, regardless of a claim's legal merits. It discusses how OSPs are likely to interpret the law's requirements in practice, as well as alternate interpretations that could be advanced to better protect online expression. Section III.D reviews the law's free expression provisions and identifies important shortcomings. Finally, Section III.E discusses the law's extraterritorial application to information created and shared outside of the EU.

Cumulatively, these GDPR provisions make RTBF claims uniquely powerful legal tools—both for legitimate claimants and for abusive ones targeting information the public has a right to see.¹⁵⁸ A person asserting a

157. *Id.* art. 85; *see also infra* Section III.D (discussing Article 85); William Long & Francesca Blythe, *Member States' Derogations Undermine the GDPR*, PRIVACY L. & BUS. U.K. REP., May 2016, at 10 (discussing other Member State powers under the GDPR).

158. Given the unique power of RTBF claims, it is possible that in the future they could displace claims such as defamation, becoming the primary legal tool for individuals to control

RTBF claim can bypass long-standing laws and substantive legal defenses that would have shielded lawful speech against other claims based on reputational harms, such as defamation or invasion of privacy.¹⁵⁹ As Professor Joris van Hoboken has pointed out, these well-established laws already address many of the problems covered by RTBF claims, and entail “intricate doctrines to balance the interests in society in the publicity of and about others and the interests of privacy and dignity of natural persons.”¹⁶⁰

The GDPR’s notice-and-takedown rules also appear to provide RTBF claimants with great procedural advantages compared to other notice-and-takedown claimants, as Section III.C details. Later, Part IV proposes a way to restore balance in this regard, by applying law under the EU’s eCommerce Directive. That approach could preserve the GDPR’s pro-privacy goals while avoiding many of the harms to online speech described here.

A. UNCLEAR RULES AND ONE-SIDED INCENTIVES

It is hard to read the GDPR, and that is a problem. Even data protection experts cannot say for sure how the GDPR answers hugely consequential questions, like whether hosting platforms must carry out RTBF removals.¹⁶¹ It is even harder to parse the detailed provisions affecting notice-and-takedown operations. The Regulation’s ambiguous requirements, coupled with its incentive structure for OSPs, will systematically push toward acceptance of overreaching removal requests.

what others can say about them online. Claims brought by government, commercial, or other non-individual interests—including most intellectual property claims—would likely continue to rely on other laws.

159. See Gabrielle Guillemin, *Advisory Council to Google on the RTBF - London Meeting 16th October 2014*, GOOGLE ADVISORY COUNCIL (Oct. 16, 2014), https://docs.google.com/document/d/1kI269r0gW7lmvpe4ObRvRB_-68JN2yRSb-g2s3JD9qo/pub [<https://perma.cc/2QMZ-A2U4>] (testifying about concern that “the line between data protection, privacy and defamation is becoming unhelpfully blurred”); *NT 1 & NT 2 v. Google*, [2018] EWHC 799 (QB) (rejecting the argument that the claimant abused legal process by bringing a RTBF claim instead of a defamation claim, but applying standards grounded in defamation and putting the burden of proof on the RTBF claimant); Iain Wilson, *NT1 and NT2 v Google Inc: How to Seek the Delisting of Search Engine Results Following the First English Decision on the “Right to Be Forgotten”*, INFORMM’S BLOG (Apr. 20, 2018), <https://informm.org/2018/04/20/nt1-and-nt2-v-google-inc-how-to-seek-the-delisting-of-search-engine-results-following-the-first-english-decision-on-the-right-to-be-forgotten/> [<https://perma.cc/Z3MB-R48Z>] (summarizing the decision and its implications).

160. JORIS VAN HOBOKEN, *THE PROPOSED RIGHT TO BE FORGOTTEN SEEN FROM THE PERSPECTIVE OF OUR RIGHT TO REMEMBER* 23 (2013), http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscrypt_2013.pdf [<https://perma.cc/U5AD-DL2V>].

161. See *infra* Section III.B.

It is generally accepted that the rule of law requires “the effect of community legislation [to] be clear and predictable for those who are subject to it.”¹⁶² As the U.S. Supreme Court has described the analogous problem under U.S. law, unclear speech regulations may cause citizens to “steer far wider of the unlawful zone . . . than if the boundaries of the forbidden areas were clearly marked.”¹⁶³ Where laws affect free expression rights under the European Convention, the requirement of predictable meaning is particularly stringent.¹⁶⁴

The risk that lawful speech will be suppressed through cautious overcompliance is increased when an OSP—rather than a speaker or information seeker—decides how to interpret an unclear regulation affecting the latter’s rights. This concern about OSPs’ overcompliance in blocking lawful information is sufficiently serious that, in a case involving an unclear judicial injunction, the CJEU required that Internet users be permitted to challenge overblocking in court.¹⁶⁵

For each ambiguity in the GDPR, there are clear incentives for OSPs to err on the side of protecting the requester’s data protection rights, rather than other Internet users’ expression rights. A brief review of the GDPR will tell companies that they face fines as high as twenty million euros,¹⁶⁶ easily dwarfing the risk from most legal takedown demands, including the €130,000 (\$150,000) potentially at stake for U.S. DMCA copyright removals.¹⁶⁷

162. Joined Cases 212 to 217/80, *Amministrazione delle Finanze dello Stato v. Salumi*, 1981 E.C.R. 2735, 2751 ¶ 10; see also *Annexes to the Communication from the Commission to the European Parliament and the Council: A New EU Framework to Strengthen the Rule of Law*, COM (2014) 158 final (Mar. 11, 2014), http://ec.europa.eu/justice/effective-justice/files/com_2014_158_annexes_en.pdf [<https://perma.cc/JRM9-T7GH>].

163. *Baggett v. Bullitt*, 377 U.S. 360, 372 (1964) (quoting *Speiser v. Randall*, 357 U.S. 513, 526 (1958)).

164. See European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 10.2, 213 U.N.T.S. 221 (explaining that restrictions on free expression violate fundamental rights unless “provided by law”); *Yildirim v. Turkey*, App. No. 3111/10, Eur. Ct. H.R. ¶ 57 (2012) (holding that the “prescribed by law” standard requires a law be “formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct”). Some might argue that so long as the RTBF involves only de-listing, rather than erasure, the law does not restrict speech and thus this standard does not apply. See *infra* Section III.B.

165. Case C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*, 2014 EUR-Lex CELEX LEXIS 62012CJ0314 ¶ 54 (Mar. 27, 2014).

166. GDPR, *supra* note 6, art. 83(5). The GDPR also provides for damages to the harmed data subject. *Id.* art. 82.

167. 17 U.S.C. § 504(c)(2) (2012). As of 2016, the largest data protection fine authorized in the UK was about £500,000 (€570,000) and the largest fine actually assessed was about £250,000 (€285,000). HUNTON & WILLIAMS, *supra* note 145, at 12.

OSPs that contact DPAs or are able to obtain expert counsel will almost certainly be advised not to worry about fines of this magnitude. The GDPR requires that fines be “effective, proportionate and dissuasive,” and few expect regulators to punish data controllers that act in good faith.¹⁶⁸ But it is unrealistic to expect most OSPs to know this—particularly if they come within the GDPR’s jurisdictional scope but have no experience with EU law. A growing startup in India or Brazil with hopes of expanding into European markets, for example, has reason to avoid legal trouble there, and little ability to ascertain whether a RTBF request is legally valid.

For larger and more sophisticated OSPs, the sheer number of RTBF requests—each one posing a separate risk of penalties, bad press, or damaged relationships with DPAs if the OSP fails to remove content—may create similar pressures. Incentives to overcomply may be reinforced by fear of attention from data protection regulators. Once a company is under review, it could be found noncompliant with the GDPR’s other rules and subject to additional fines or even requirements to redesign its products.¹⁶⁹ Companies unsure of their status as processors or controllers may also hesitate to challenge RTBF claims, since being deemed controllers would add significantly to their compliance obligations.¹⁷⁰

As a practical matter, the best or most accurate interpretation of the GDPR will not be the one that shapes outcomes for Internet users. What matters in most cases will be the interpretations OSPs follow in practice, given unclear rules, high potential penalties, and minimal transparency or public review. This practical backdrop will affect the real-world outcome of every legal ambiguity identified in this Article.

B. RIGHT TO BE FORGOTTEN OBLIGATIONS FOR HOSTS AND SOCIAL MEDIA

One of the biggest open questions about the new RTBF provisions is whether they apply to hosting platforms. Hosts—ranging from large commercial operations like Facebook or DailyMotion to local news forums—store content uploaded by users, typically making it accessible to other people

168. GDPR, *supra* note 6, art. 83(1). This expectation also comes from the author’s discussions with EU data protection practitioners, who predicted that the high fines authorized in the GDPR would be used only in cases of extreme intransigence, and noted DPA officials’ professionalism and commitment to fair and reasonable interpretations of the law.

169. *See infra* Section III.E (explaining that DPAs can also carry out far-reaching audits of regulated companies, including compelling the production of information and documents); GDPR, *supra* note 6, art. 58.

170. *See supra* Section II.B.

online. Hosts support a tremendous amount of speech by ordinary Internet users.¹⁷¹ That expression will be threatened if the GDPR's new RTBF rules apply to it. As this Section will discuss, this is an open legal question. There are arguments against requiring hosts to honor RTBF requests on the basis that they are only processors following the instructions of users, who are themselves the controllers of uploaded data. But the real-world motivation of the actors involved, including both OSPs and regulators, may nonetheless push hosts toward RTBF removals.

Doctrinally, the existence of RTBF obligations should turn on whether a host counts as a controller, which is defined in the GDPR as an entity that “determines the purposes and means of the processing of personal data.”¹⁷² As discussed in Section II.C, classifying hosts as controllers raises real problems, seemingly subjecting them to obligations they cannot fulfill. The scant case law applying *Google Spain* to hosting platform defendants to date has not clarified matters. At least one court has held that a host—Google's Blogger service—was a processor, not a controller, for material uploaded by its users.¹⁷³ At least one other court has accepted that Facebook was a controller.¹⁷⁴ And a third court (in a pre-*Google Spain* ruling), held that a host was a controller at some times but not at others.¹⁷⁵

171. See, e.g., Sirena Bergman, *We Spend a Billion Hours a Day on YouTube, More than Netflix and Facebook Video Combined*, FORBES (Feb. 28, 2017, 7:32 AM), www.forbes.com/sites/sirenabergman/2017/02/28/we-spend-a-billion-hours-a-day-on-youtube-more-than-netflix-and-facebook-video-combined/ [https://perma.cc/7JWS-9E9P] (reporting that YouTube receives “around 400 hours of content every minute, from creators all over the world”).

172. GDPR, *supra* note 6, art. 4(7). The Article 29 Working Party's 2010 opinion identified some but not all hosts as controllers under the similar standards of the 1995 Directive. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 84, at 25; see also VAN HOBOKEN, *supra* note 160, at 8 (discussing complexity of assessing controller status for social media OSPs).

173. See *Google Spain, SL v. Agencia Protección de Datos, S.A.N.*, Dec. 29, 2014 (R.J., No. 70) (Spain), <http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7309398&links=28079230012014100466&optimize=20150302&publicinterface=true> [https://perma.cc/525J-9DHM], *rev'd on other grounds*, Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317; Miquel Peguera, *Spain: The Right to Be Forgotten Does Not Apply to Blogger*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y (Mar. 4, 2015, 9:01 AM), <http://cyberlaw.stanford.edu/blog/2015/03/spain-right-be-forgotten-does-not-apply-blogger> [https://perma.cc/HL7W-XEEU]; Miquel Peguera, *Clash Between Different Chambers of the Spanish Supreme Court on the Right to Be Forgotten*, ISP LIABILITY (Apr. 11, 2016), https://ispliability.wordpress.com/2016/04/11/clash_bewteen_different_chambers/ [https://perma.cc/U698-44RK].

174. *CG v. Facebook Ireland Ltd* [2016] NICA 54, ¶¶ 88, 91, 96 (Nor. Ir.), www.bailii.org/nie/cases/NICA/2016/54.html [https://perma.cc/AYW9-46U2].

175. Corte di Cassazione, Cass. sez. tre Penale, 3 febbraio 2014, n. 5107/14 (It.), http://www.dirittoegustizia.it/allegati/15/0000063913/Corte_di_Cassazione_sez_III_Penale_sentenza_n_5107_14_depositata_il_3_febbraio.html [https://perma.cc/XX52-T5XS]; see also *infra* Section IV.B (discussing this case).

The *Google Spain* opinion does not tell us whether the RTBF applies to hosts, but it provides some important clues. The court's analysis focuses on a form of processing unique to web search engines: generating search results, aggregated from different sources across the web, to create a "more or less detailed profile" of an individual.¹⁷⁶ The court said that this *de facto* profile was "liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page."¹⁷⁷

This focus on search results shaped the *Google Spain* remedy. The court required Google to remove data from "the list of results displayed following a search made on the basis of a person's name,"¹⁷⁸ but Google did not have to delete its own hosted copies of the data or delete the same results for other search queries.¹⁷⁹ This is less than plaintiff had asked for: he wanted to completely "prevent indexing of the information relating to him personally," so that it would "not be known to internet users."¹⁸⁰

The court also emphasized that, when the law requires a search engine to erase links to a page, that does *not* mean that data on the underlying web page must also be erased.¹⁸¹ This was the case for the Spanish newspaper page at issue in *Google Spain*.¹⁸² The court distinguished Google from the website based on the latter's potentially stronger "legitimate interests justifying the processing . . ."¹⁸³ Preserving information on web pages—whether self-published or hosted—protects expression and information rights in particular. Indeed, data protection regulators have said that Google delistings do not significantly threaten these rights precisely *because* information is still available on the webpage.¹⁸⁴ Many free expression advocates may disagree, as a prominent library association did, arguing that "if certain search results are hidden or removed from search results, this has much the same effect as

176. See Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317, ¶ 37.

177. See *id.* ¶¶ 80, 87.

178. *Id.* ¶ 88.

179. *Id.*

180. *Id.* ¶ 20.

181. *Id.* ¶¶ 82–88. The website in *Google Spain* was a news site eligible for special journalistic protections, but with respect to the data at issue in the case it effectively acted as an intermediary—publishing content created by the government and at the direction of the government, rather than publishing its own reporting. See Peguera, *supra* note 5, at 523 n.70, 524 n.74.

182. *Google Spain*, 2014 E.C.R. 317, ¶¶ 82–88.

183. *Id.* at ¶ 86.

184. See ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 2.

deleting the original content,” given users’ difficulty in finding it without a search engine.¹⁸⁵

Whatever the informational harms of search delisting, it is clear that the harms from requiring hosts to erase content are more serious. Deleting information from a hosting site may eliminate it from the Internet completely. It may also eliminate the author’s only copy. As human creative output moves online, users increasingly rely on hosts—from cloud storage providers to social media companies—to store their work.¹⁸⁶ Erasing the hosted copy could delete all traces of the author’s expression—a drastic remedy, and one that has been rejected by the ECHR in other situations even for clearly unlawful material.¹⁸⁷

Following *Google Spain*, one possible conclusion is that hosts cannot have RTBF obligations because they do not carry out the kind of “profiling” that triggered RTBF obligations for Google. The balance of rights and interests identified by the court also plays out very differently for hosts: they typically create lesser privacy harms for data subjects,¹⁸⁸ and serve a more essential role for expression and information rights.¹⁸⁹ If Twitter deleted the tweet about

185. Letter from Gerald Leitner, Sec’y Gen., Int’l Fed’n of Libr. Ass’ns & Insts., Application of Right to be Forgotten Rulings: The Library Viewpoint (Oct. 24, 2016), http://www.ifla.org/files/assets/faife/statements/161024_ifla_on_rtbf_case_in_france.pdf [<https://perma.cc/8BSC-6ZLC>].

186. In 2016 an artist reported that Google had deleted fourteen years of his work, including his only copies of some pieces, by taking down content he had posted to the company’s Blogger service. Fiona Macdonald, *Google’s Deleted an Artist’s Blog, Along with 14 Years of His Work*, SCI. ALERT (July 18, 2016), <http://www.sciencealert.com/google-has-deleted-an-artist-s-blog-with-14-years-of-his-work> [<https://perma.cc/7LEZ-EESJ>]. Similar experiences could easily occur for ordinary Internet users who, for example, rely on Facebook to retain photographs uploaded from their phones.

187. *Węgrzynowski & Smolczewski v. Poland*, App. No. 33846/07, Eur. Ct. H.R. (2013), <http://hudoc.echr.coe.int/eng?i=001-122365> [<https://perma.cc/8M3S-LFEF>] (holding that news articles held defamatory should not be purged from archives and that other remedies such as annotation suffice). The court wrote: “The Court accepts that it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations.” *Id.* ¶ 65. The idea that even illegal writings should be preserved for experts or posterity has an interesting history in the German library tradition of the *Giftschrank* or poison cabinet—a storage place for banned books, many of which were later restored to circulation. See Sam Greenspan, *The Giftschrank*, 99% INVISIBLE (Mar. 8, 2016), <http://99percentinvisible.org/episode/the-giftschrank/> [<https://perma.cc/QT7Z-HRTP>].

188. *Google Spain*, 2014 E.C.R. 317, ¶ 80 (explaining that web search results significantly impact privacy because they enable “any internet user to obtain through the list of results a structured overview of the information” about the data subject).

189. *Id.* ¶ 86 (noting that the balance of interests may be different for search engines and webmasters “given that, first, the legitimate interests justifying the processing may be different

Matilda Humperdink’s food making diners sick, for example, people might have no other warning about the risk to their health.

Another possible interpretation is that hosts trigger RTBF obligations when they let users search hosted content for names, generating a search result “profile” based on content stored on the host’s servers.¹⁹⁰ If that were correct, and if Twitter were a controller, it would not have to delete the tweet about Matilda Humperdink—but it might have to delist it from results in Twitter’s search box. The Article 29 Working Party disapproved of this interpretation in its *Google Spain* guidelines, saying that “[s]earch engines included in web pages” generally should not be subject to any delisting obligation.¹⁹¹

A final possibility is that hosts have some form of RTBF duties, but that they are limited compared to those of search engines because of the different balance of rights. This could mean any number of things in practice. At a minimum, hosts would comply with fewer RTBF requests because, under *Google Spain*, a website can legitimately process data even when a search engine may not.¹⁹² For example, Google might have to delist the Matilda Humperdink tweet, while Twitter might be able to leave it up.

In summary, no one knows whether the RTBF applies to hosts, and no one knows what hosts’ erasure obligations would look like if it did. Like other open questions in the GDPR, this one is a problem precisely because it is open, leaving both regulators and OSPs relatively unconstrained in their interpretations.

As a practical matter, hosts that receive RTBF requests will have two options. One is to keep the challenged content online, and risk being summoned before a DPA. If the DPA decides that the host is a controller, then the host will face not only RTBF obligations, but also the daunting array of other requirements applicable to controllers. The host’s other option is to acquiesce to the RTBF request and avoid this risk. In the absence of

and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same”).

190. *Id.* ¶ 33 (identifying the creation of a search results “profile” as a harm that supported the case outcome). Setting a higher threshold for legal claims against hosts may be counterintuitive to intermediary liability specialists in areas such as copyright, since OSPs typically face greater liability for hosting content and lesser liability for merely linking to it. *See, e.g., Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1161–62 (9th Cir. 2007) (holding that copyright is not infringed by inline linking and framing because the content was not hosted by the defendant). Those cases are different because they turn on whether a link creates any liability at all—they do not address the question, posed here, about substantive standards to apply when balancing claimants’ rights against those of other people.

191. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 8.

192. *Google Spain*, 2014 E.C.R. 317, ¶ 80; *see also infra* Section III.C.3 (discussing erasure standards and technical implementations for hosts).

meaningful transparency requirements, a host could do so inconspicuously, without acknowledging any controller status or legal obligation, by saying the removal was voluntary.¹⁹³

DPA's, meanwhile, have institutional incentives to favor RTBF obligations for hosts. Classifying hosts as controllers increases the effective authority of DPAs and gives them means to help genuinely aggrieved people.¹⁹⁴ The political calculus thus favors deeming hosts controllers when the opportunity arises.

As a practical matter, then, controller status for hosts may be inevitable. Many questions (*a host* of questions, you might say) will then arise about how the substantive and procedural RTBF rules for hosts may differ from the ones for search engines.

C. NOTICE-AND-TAKEDOWN PROCESS

This Section will walk through an intermediary's steps in response to a RTBF request. In some respects, these steps resemble the standard notice-and-takedown process that would apply to other claims, such as defamation. In important details, however, the GDPR provides new rules that systematically favor the rights of claimants asserting data protection rights over those of other Internet users.

These steps are not laid out in a single section of the Regulation, but can be cobbled together from various provisions—many of which are ambiguous. Some are not spelled out but can be inferred from regulators' interpretations of similar provisions in pre-GDPR law. The steps are generally sensible for back-end data removals, such as requests to delete accounts, logs, or profiles. They are, however, unreasonable when applied to online expression, threatening both the information and privacy rights of Internet users.¹⁹⁵

Following the GDPR's apparent requirements, an OSP would follow these steps.¹⁹⁶ Each is discussed in detail in this Section.

193. An important step toward codifying better transparency practices in such situations comes from the second conference on Content Moderation at Scale, which produced the Santa Clara Principles. *See Santa Clara Principles on Transparency and Accountability in Content Moderation*, (May 7, 2018), https://newamericadotorg.s3.amazonaws.com/documents/Santa_Clara_Principles.pdf [<https://perma.cc/EM98-N2HH>] [hereinafter SANTA CLARA PRINCIPLES].

194. Regardless of the host's controller status, people with valid claims such as defamation could still get judicial relief.

195. *See infra* Section II.C.

196. *See also* Kuczerawy & Ausloos, *supra* note 5, at 236–46 (discussing EU intermediary liability law considerations for the *Google Spain* removal process, including issues of transparency and webmaster notice).

1. The OSP receives a RTBF request, and perhaps communicates further with the requester to clarify what is being sought.¹⁹⁷
2. If the data subject requests it, the OSP may temporarily suspend or “restrict” the content so it is no longer publicly available—before actually assessing the erasure request.¹⁹⁸
3. The OSP assesses the RTBF request to decide if it states a valid claim for erasure. For difficult questions, the OSP may be allowed to consult with the user who posted the content.¹⁹⁹
4. For valid claims, the OSP delists or erases the content. For invalid claims, it may bring the content out of “restriction” and reinstate it to public view.²⁰⁰
5. The OSP informs the requester of the outcome and communicates the removal request to other controllers processing the same data.²⁰¹
6. If the data subject requests, the OSP discloses any contact details or identifying information about the user who posted the now-removed content.²⁰²
7. In most cases, the OSP is not allowed to tell the accused user that content has been delisted or erased, and can give the user no opportunity to object.²⁰³
8. The OSP can publicly disclose aggregated or anonymized information about removals, but not individual instances.²⁰⁴

For each of these steps, an OSP’s safest interpretation of the GDPR tilts the scales toward removal, and against procedural or substantive rights for the other people whose rights are affected.

197. GDPR, *supra* note 6, art. 17; *infra* Section III.C.1.

198. GDPR, *supra* note 6, art. 18; *infra* Section III.C.2.

199. GDPR, *supra* note 6, arts. 17(1), 21; *infra* Section III.C.3.a.

200. GDPR, *supra* note 6, arts. 17, 18, 21; *infra* Section III.C.3.b.

201. GDPR, *supra* note 6, arts. 12(3), 17, 19; *infra* Section III.C.4.a.

202. GDPR, *supra* note 6, arts. 14(2)(f), 15(1)(g); *infra* Section III.C.4.b.

203. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 3; *infra* Section III.C.4.c.

204. *See infra* Section III.C.4.d.

1. Removal Requests

The notice-and-takedown process begins when the data subject requests “erasure” or “objects to the processing” of personal information.²⁰⁵ The data subject can ask the OSP to “restrict” processing by taking the data offline, “erase” the data, or both. The GDPR does not specify what information the requester must provide to set the removal process in motion. This omission, if left uncorrected, will make the process slower and less predictable for both the requester and the OSP. Clear form-of-notice requirements help claimants submit actionable requests on the first try and tell them when the ball is in the OSP’s court to respond.²⁰⁶ For example, if Matilda wants the tweet erased, she should have to tell Twitter basic information like the tweet’s URL, and hopefully also disclose any public interest in the tweet’s contents by telling Twitter she operates a chain of fast-food restaurants. Without formal requirements, notice-and-takedown requests commonly omit such information.²⁰⁷

Form-of-notice requirements also tell the OSP when the request is procedurally valid, and the burden has shifted to it to begin substantive review. The GDPR requires that OSPs complete this review within one month in most cases. Importantly, though, it is not clear if the clock starts ticking at the moment the request arrives, or once the intermediary has enough information to meaningfully evaluate the request.²⁰⁸ A risk-averse OSP will assume the former, and rush to process even a poorly substantiated request.

The GDPR does allow the OSP to ask for identification if there is a reasonable doubt as to the data subject’s identity.²⁰⁹ This extra precaution is important, and OSPs should take on the expense and nuisance of doing it to prevent imposters from taking down information about other people. OSPs

205. GDPR, *supra* note 6, arts. 17(1), 17(1)(c). The separate erasure and objection rights contained in Articles 12 and 14 of the 1995 Directive reappear in altered form as GDPR Articles 17 and 21. The relationship between the two rights is complex. See Jef Ausloos, *The Interaction Between the Rights to Object and to Erasure in the GDPR*, KU LEUVEN CTR. FOR IT & IP L. (Aug. 25, 2016), <https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/> [<https://perma.cc/C3L4-TX6N>].

206. The Article 29 Working Group’s *Google Spain* guidelines for removals contain sensible form-of-request requirements, calling for RTBF requesters to “sufficiently explain the reasons why they request de-listing, identify the specific URLs and indicate whether they fulfill a role in public life, or not.” ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 7. Bing’s RTBF removal form also sensibly asks about the claimant’s role in public life. *Request to Block Bing Search Results in Europe*, BING, <https://www.bing.com/webmaster/tools/eu-privacy-request> [<https://perma.cc/36WH-MCL7>] (last visited Mar. 31, 2018).

207. URBAN ET AL., *supra* note 19.

208. GDPR, *supra* note 6, art. 12(3).

209. *Id.* art. 12(6).

may also reject requests that are “manifestly unfounded or excessive, in particular because of their repetitive character.”²¹⁰

2. Temporarily “Restricting” Content

The next step is a striking departure from notice-and-takedown legal norms: data subjects can instruct data controllers to immediately “restrict” public access to information, taking it offline *before* determining whether the RTBF erasure request is valid.²¹¹ This provision could compel OSPs to block access to blog posts, tweets, search results, and other user-generated information—even for claims that later prove to have no basis in law.²¹² In some cases, this temporary removal could deprive Internet users of vitally important information—for example, about a corrupt politician on the eve of election; an embezzler meeting a new client; or a convicted abuser looking for a date. But even outside these scenarios where the timing is critical, applying restriction requirements to online expression raises grave concerns. Claimants may request restriction for almost any RTBF request, and the bases for OSPs to push back on that request are extremely unclear.

a) Triggers for Restriction

The GDPR lists several situations in which data subjects can compel controllers to “restrict” content. One is when “the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify” its truth.²¹³ So, for example, Matilda could invoke this provision by claiming the tweet about her is false. This is a remarkable shift from the rules that would protect online expression against an identical claim of falsity under defamation and ordinary intermediary liability laws.²¹⁴ As applied to OSPs, this provision is also wildly impractical. OSPs have no reasonable means to “verify the accuracy of the personal data” in communications like a tweet. Twitter does not know if Matilda really hosted a dinner or got sick, and probably does

210. *Id.* art. 12(5). An intermediary that rejects a request on this basis assumes the burden of proof for its conclusion. *Id.*

211. *Id.* art. 18. The GDPR’s pre-removal restriction requirement has no analog in any major intermediary liability law, including the U.S. DMCA and the EU eCommerce Directive. See 17 U.S.C. § 512 (2012); *supra* Section II.A (discussing the EU eCommerce Directive’s “knowledge” standard). These laws typically give OSPs a window of time to assess the allegation and reach a reasoned decision.

212. This problem intersects with the lack of form-of-notice requirements discussed in Section III.C.1: if a requester can get information restricted without even providing information adequate to permit substantive review of her claim, the potential for abuse is particularly high.

213. GDPR, *supra* note 6, art. 18(1)(a).

214. See *supra* Section II.A; Guillemin, *supra* note 159.

not even know if she is a real person. If restricted information can be reinstated only once an OSP has somehow unearthed the facts about a real-world dispute, it will not be reinstated.²¹⁵

Another basis for restriction under the GDPR applies in situations where the controller's initial basis for processing data was based on "legitimate interests."²¹⁶ As discussed in Section II.C, the "legitimate interests" basis underlies almost all OSP processing of user-generated content. Thus, this provision lets claimants demand restriction for practically any RTBF request. Restricted content stays offline pending an OSP's later, and final, evaluation of the erasure request. Such content may,

[W]ith the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.²¹⁷

The scope of the exception for protection of other people's rights is, as will be discussed in the next Section, unclear.

b) Exceptions to Restriction

When can an OSP reject a restriction request and keep content online for "the protection of the rights of another natural or legal person"?²¹⁸ One possible answer is: every time. Essentially all RTBF requests affect someone's rights to seek and impart information, and arguably her rights to procedural fairness in the face of state-mandated action. OSPs that restrict content based

215. The Article 29 Working Party's *Google Spain* guidelines suggest that not even DPAs should try to resolve disputed facts, because, although competent to assess data protection issues, they are generally "not empowered and not qualified to deal with information that is likely to constitute . . . slander or libel," and should refer the issue to courts. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 17.

216. *See* GDPR, *supra* note 6, art. 18(1)(d). This rule must be pieced together from several sections of the Regulation. OSPs that are regulated by the GDPR may lawfully process personal data "only if and to the extent that" one of six justifications applies. *Id.* art. 6(1). The justification for OSPs processing user-generated content that refers to another person is usually 6(1)(f), which allows "processing [that] is necessary for the purposes of the legitimate interests pursued by the controller or by a third party . . ." *Id.* art. 6(1)(f). A data subject can object to any processing that is done based on this 6(1)(f) "legitimate interests" justification, by invoking rights under GDPR Article 21(1). *Id.* art. 18(1)(d). If she objects "pursuant to Article 21(1)," then she can compel a controller to restrict the data subject to the weighing analysis mandated by Article 18.1(d). *Id.*

217. *Id.* art. 18(2); *see also id.* art. 4(3) (defining "restriction of processing" as "the marking of stored personal data with the aim of limiting their processing in the future").

218. Another potential basis is Article 12(5) of the GDPR, which says that an intermediary may "refuse to act" on requests that are "manifestly unfounded or excessive." *Id.* art. 12(5).

on a bare allegation suppress expression before even deciding whether the claimant's rights outweigh those of other Internet users. This includes several rights that the GDPR identifies "in particular" as important to balance with data protection, including "freedom of expression and information . . . [and] the right to an effective remedy and to a fair trial."²¹⁹ Given this impact, OSPs might be justified in routinely rejecting restriction requests that apply to other users' online expression.

The other possibility is that OSPs must apply the "protection of the rights of another natural or legal person" standard to restriction requests on a case-by-case basis. If so, the meaning of the standard is far from clear. Logically, it must mean something different from the standard for actual erasure—which, as discussed in the next Section, requires "compelling legitimate grounds" to keep the content online.²²⁰ The practical difference between these two standards is difficult to identify.

The GDPR restriction requirement shifts an important burden. Instead of an accuser having to say why expression should be prohibited—as should be required under the eCommerce Directive's "knowledge" standard for OSP removal, or in court—the GDPR gives the *OSP* the burden to identify reasons it should be permitted. Importantly, OSPs that believe they have, or even might have, the burden of proof will be less likely to stand up for users' expression rights.

3. *Permanently "Erasing" Content*

The intermediary now comes to the crux of the issue: determining whether to erase the content and carrying out the erasure.²²¹ The GDPR's guidance on both steps is unclear.

a) Deciding if Removal Is Appropriate

The criteria for this decision rest on the already-overburdened idea of "legitimate" interests. In various sections, the law tells OSPs to honor erasure requests unless:

- There are "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject;"²²²

219. *Id.* recital 4.

220. *Id.* art. 21(1).

221. *Id.* art. 17(1) ("[T]he controller shall have the obligation to erase personal data without undue delay . . .").

222. *Id.* art. 21(1). Other grounds for declining to erase data are listed in Article 21.1 and in Article 17.3, but few are likely to apply in the RTBF context.

- There are “overriding legitimate grounds for the processing;”²²³ or
- Keeping the content available is necessary “for exercising the right of freedom of expression and information.”²²⁴

How are OSPs to know what these standards mean for RTBF requests? Search engines can look to the slowly developing body of law and guidance for their unique “de-listing” obligations under *Google Spain*.²²⁵ Assuming the GDPR does not alter that standard, they can continue to apply the same rules.²²⁶

But other OSPs, including social media and other hosting platforms, have no comparable guidance.²²⁷ They should not apply rules developed for search engines: it should be *harder* to get content removed from a hosting platform, because the balance of rights and interests is different.²²⁸ Even if Google has to remove the tweet about Matilda, for example, Twitter might lawfully continue hosting it.

223. *Id.* art. 17(1)(c).

224. *Id.* art. 17(3)(a).

225. See Peguera *supra* note 5, at 557–59 (citing cases); Kulk & Borgesius, *supra* note 132, at 117–23 (same). Regulatory guidance includes the Article 29 Working Group’s *Google Spain* guidelines. See, e.g., ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103. Search engines may also, according to the Article 29 Working Party, consult with the “original editor” of the information in difficult cases. *Id.* at 3. As will be discussed *infra* Section III.C.4.c), however, this exception has limited practical value.

226. There are interesting minor deviations between the GDPR and the 1995 Directive interpreted in *Google Spain*, raising the question whether requirements—such as search engines’ removal obligations—under that case have changed. For example, the GDPR does not repeat the court’s “preponderant interest of the general public” standard for rejecting RTBF requests. Compare Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317, ¶¶ 97, 99 (using the “preponderant interest of the general public” standard), with GDPR, *supra* note 6, art. 17(1)(c) (requiring “overriding legitimate grounds” for rejection), and *id.* art. 17.3 (enumerating specific grounds for rejecting RTBF requests), and *id.* art. 21(1) (requiring “compelling legitimate grounds . . . which override the interests, rights and freedoms of the data subject” in order to reject a request).

227. Guidance about “legitimate” data processing exists, but rarely involves weighing the expression rights of absent parties. See, e.g., ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 06/2014 ON THE NOTION OF LEGITIMATE INTERESTS OF THE DATA CONTROLLER UNDER ARTICLE 7 OF DIRECTIVE 95/46/EC at 29–43 (2014), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [<https://perma.cc/P9QU-DY47>] (discussing obligations of OSPs processing back-end user data, but not online expression). Cases balancing rights to expression versus privacy also exist—but those rarely involve data protection, or set out rules for OSPs, as opposed to ordinary publishers or speakers. See, e.g., *von Hannover v. Germany*, App. No. 59320/00, Eur. Ct. H.R. ¶¶ 64–73 (2004), <http://hudoc.echr.coe.int/eng?i=001-61853> [<https://perma.cc/R35R-6X3R>] (discussing privacy rights of public figures).

228. *Supra* Section III.B.

b) Technical Implementation of “Erasure”

Once an OSP controller ascertains that a request is valid, it must “erase” the targeted content.²²⁹ The word “erase” is not defined in the GDPR. But the 1995 Directive also requires “erasure,” and the CJEU in *Google Spain* interpreted it to mean something relatively limited: de-listing from web search results for the data subject’s name, but erasing data entirely from the search index.²³⁰ If “erase” has this nuanced, term-of-art meaning for search engines, perhaps it could be interpreted flexibly for other OSPs as well.

Arguably the court’s limited erasure remedy is derived from flexible language in Articles 12 and 14 of the 1995 Directive,²³¹ which require controllers to honor objections only “as appropriate” and erase data only on “compelling legitimate grounds.”²³² In *Google Spain*, the court considered these obligations discharged when Google suspended some, but by no means all, of its processing activities using Mr. Costeja’s data.²³³ If this analysis of the doctrinal basis for the court’s remedy is correct, then the GDPR provides the same latitude for partial, tailored implementation of “erasure.” It requires controllers to erase only to the extent that there are “no overriding legitimate grounds” to continue processing.²³⁴

This interpretation creates a doctrinal basis for tailoring erasure obligations of other controllers, including hosts. Much as Google had legitimate grounds to continue some, but not all, of its processing, hosts may have grounds to continue some of theirs. The doctrinal flexibility that led the CJEU to its *Google Spain* remedy could lead to equally tailored erasure obligations for those OSPs. For example, as discussed above, a host might “erase” information solely from results of its own on-site or in-app search function.²³⁵ Or a social network

229. GDPR, *supra* note 6, art. 17(1).

230. See 1995 Directive, *supra* note 69, art. 12; *Google Spain*, 2014 E.C.R. 317, ¶ 3.

231. See Daphne Keller, *Global Right to Be Forgotten Delisting: Why CNIL Is Wrong*, STAN. L. SCH. CTR. FOR INTERNET & SOC’Y (Nov. 18, 2016, 12:59 AM), <http://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong> [<https://perma.cc/XXH5-JCQV>].

232. See 1995 Directive, *supra* note 69, art. 12(b) (“[T]he right to obtain from the controller . . . as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive”); *id.* art. 14(a) (“[T]he right . . . in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds . . . to the processing of data relating to him Where there is a justified objection, the processing instigated by the controller may no longer involve those data.”).

233. *Google Spain*, 2014 E.C.R. 317, ¶ 82.

234. GDPR, *supra* note 6, art. 17(1)(c).

235. See *supra* Section III.B. Hosts could also justify maintaining copies of “erased” expression by reference to Article 17(3)(e), which excuses controllers from erasing data “to the extent that processing is necessary” for the “establishment, exercise or defence of legal

might change settings to make a public post visible only to friends or followers, or prevent “viral” spread of information by making it harder to share a particular video within the network. This leaves the technical implementation of RTBF erasure under the GDPR very much up in the air, and open to thoughtful, tailored solutions based on balancing affected parties’ rights.

4. *Transparency*

Transparency provides one of the most important checks against flawed notice-and-takedown processes. When data subjects and other affected people know about a removal decision, they can identify and challenge both over-removal and under-removal. Transparency to the public, including academics, regulators, and civil society, helps correct both kinds of mistakes and allows tracking of larger scale trends and problems.²³⁶ The GDPR permits some limited transparency, but not enough to serve all these purposes. In some cases, it seems to mandate transparency that compromises speakers’ own data protection rights, under terms that seem antithetical to good practice and to the GDPR’s stated goals.

a) Telling Controllers and the Requester

The OSP must, reasonably, inform the requesting data subject when it erases information or otherwise takes action based on a removal request.²³⁷ It is also responsible for conveying information about the request to others who may be processing the data.²³⁸ This obligation appears twice in the GDPR.²³⁹ In one version, the obligation seems to require notice only to downstream “recipient[s] to whom the personal data have been disclosed.”²⁴⁰ In the other, it applies to a seemingly broader class of any “controllers which are processing the personal data.”²⁴¹

For OSPs and their users, these requirements can lead to perverse outcomes. As an example, the webmaster who put information online in the first place would be one important “controller[] which [is] processing the same

claims.” *Id.* art. 17(3)(e). It is certainly foreseeable that legal claims, against the OSP or otherwise, could arise from RTBF erasure—particularly if a host erases a user’s sole copy of something important.

236. *See, e.g.*, Brief of Amici Curiae, *supra* note 42, at *8–9; SANTA CLARA PRINCIPLES, *supra* note 193.

237. GDPR, *supra* note 6, art. 12(3).

238. *Id.* arts. 17(2), 19. Controllers need not erase information if it “proves impossible or involves disproportionate effort.” *Id.* art. 19.

239. *Id.* arts. 17(2), 19.

240. *Id.* art. 19.

241. *Id.* art. 17(2).

data” as a search engine.²⁴² But the Article 29 Working Party has already said it thinks that Bing and Google should *not* contact webmasters in most cases.²⁴³ Similarly, Facebook may know which users liked or shared a post, or even simply viewed it. The GDPR seems to oblige Facebook to notify these people, as “recipient[s] to whom the personal data have been disclosed”—not only about erasures, but even about failed requests that led only to temporary “restriction” of online content.²⁴⁴

Few data subjects filing RTBF requests will want this additional social media attention.²⁴⁵ If these provisions apply to OSPs, they effectively take away the data subject’s freedom, emphasized by the Article 29 Working Party, to “choose how to exercise” their rights by “selecting one or several” of possible recipients for RTBF requests.²⁴⁶

These provisions are clearly better suited to traditional data controllers like a hospital that shares patient information with an outside physician. And the provisions of the GDPR seem well targeted to online actors, including OSPs, if they share back-end data about their users for purposes such as advertising. Presumably the GDPR’s drafters had these kinds of data sharing in mind. But if OSPs are deemed controllers of user-generated content, provisions like this will cover this public information, too—with perverse and unintended results.

b) Giving the Requester Personal Information About the Speaker

Another extremely odd GDPR provision is its apparent requirement that OSPs disclose personal information about users whose posts are targeted by RTBF requests.²⁴⁷ Such disclosure is seriously out of line with the GDPR’s general pro-privacy goals, and it is hard to imagine that drafters intended them to apply in the RTBF context.

The requirement appears twice. One provision requires controllers to tell the data subject “from which source the personal data originate.”²⁴⁸ Another

242. *Id.* art. 17(2); Opinion of Advocate General Jääskinen, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2013 E.C.R. 424, ¶ 40.

243. *See infra* Section III.C.4.c).

244. GDPR, *supra* note 6, art. 19 (requiring that OSPs “shall communicate any rectification or erasure of personal data or restriction of processing”).

245. They are, after all, trying to limit dissemination of their personal data.

246. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 7.

247. GDPR, *supra* note 6, arts. 14(2)(f), 15(1)(g).

248. *Id.* art. 14(2)(f). Exceptions to this obligation are listed at Article 14(5), but none would appear applicable. *See id.* art. 14(5). The most promising exception, Article 14(5)(c), excuses the controller from informing the data subject of the poster’s identity where “obtaining or disclosure is expressly laid down by Union or Member State law.” *Id.* art. 14(5)(c). It is tempting to read this to mean that an intermediary need not disclose a poster’s identity when the law protects the poster’s privacy or right to speak anonymously.

says they must provide, upon the data subject's request, "any available information as to [the data's] source . . ." ²⁴⁹ Applied to OSPs, for which the "source" of the data is an Internet user posting her expression online, these requirements make no sense.

If Twitter were deemed a controller for the tweet about Matilda Humperdink, for example, the GDPR would entitle her to "any available information" about the tweet's source—which is to say, whatever Twitter knows about the person who posted the tweet. Twitter is supposed to provide this information even if it finds no legal ground to erase the tweet. ²⁵⁰

Applied to OSPs, these rules seriously alter the landscape for anonymous expression and strip online speakers of their own data protection rights. These sections of the GDPR, like so many others, seem crafted to apply to back-end data—not online expression.

c) (Not) Telling the Person Whose Expression Was Erased

In the aftermath of the *Google Spain* ruling, the Article 29 Working Group considered whether Google should be permitted to tell webmasters when their pages were delisted. The Group opined that "[t]here is no legal basis for such routine communication under EU Data Protection law." ²⁵¹ But they said that

Unfortunately, it probably does not mean that. The 1995 Directive has similar language, requiring controllers to tell the data subject about any disclosure of her information unless "disclosure is expressly laid down by law." 1995 Directive, *supra* note 69, art. 11(2). There, "expressly laid down by law" means "required by law." As the EU Agency for Fundamental Rights explains, the idea is that controllers do not need to tell a data subject when the law requires them to disclose her information, because she is presumed to know the law. *See* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 97 (2014), http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf [<https://perma.cc/CU8L-XB2W>]. The GDPR exception seemingly means the same thing: a controller need not tell the data subject about things that, based on the law, she should already know. It is not an exception to the duty to tell her things she does not know—in particular, the identity of the person who posted information about her.

249. GDPR, *supra* note 6, art. 15(1)(g). This provision also has language that initially appears to exempt controllers from disclosing information—in this case, based on "the rights and freedoms of others." *Id.* art. 15(4). However, this only exempts controllers from sharing a copy of the processed data, not from disclosing the data's source. *See id.*

250. Arguably, Matilda could also make Twitter tell her who read the tweet. Article 14(1)(e) of the GDPR entitles her to find out "the recipients or categories of recipients of the personal data, if any . . ." *Id.* art. 14(1)(e). Similarly, Article 19 says that for "each recipient to whom the personal data have been disclosed," the controller "shall inform the data subject about those recipients if the data subject requests it." *Id.* art. 19. It is to be hoped that this relatively loose language gives OSPs leeway to tell the data subject "about those recipients" in general terms, without disclosing their individual personal information.

251. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 3.

consultation would be acceptable in unusual cases when necessary to resolve difficult requests.²⁵²

The question whether routine notice to webmasters violates the law under the 1995 Directive remains in dispute.²⁵³ In 2016, the Spanish DPA fined Google €150,000 for telling a webmaster when a page was delisted.²⁵⁴ The GDPR does nothing to clarify the issue. But because it does not appear to change any relevant law, presumably the interpretation of the Article 29 Working Group (or the new Board) will remain the same. If hosts are deemed to be controllers, the same reasoning could preclude notice to their users when online expression is deleted.

Prohibiting notice to the affected online speaker makes some sense from a pure data protection perspective. After all, the requester is exercising a legal right to make the OSP stop processing her information. A company that then talks to a poster, publisher, or webmaster about the request is continuing to process data. More pragmatically, a person whose privacy is violated by online content may not want the perpetrator to know of any removal efforts.

As a matter of procedural fairness or protection of free expression, though, taking content down based solely on an accusation—with no notice to the accused or opportunity for defense—raises obvious problems. It places the fate of online expression in the hands of accusers and technology companies—neither of whom has sufficient incentive to stand up for the speaker’s rights. That is why notice to the accused, and an opportunity to reply, is so central to many civil society standards for intermediary liability, including the widely endorsed Manila Principles.²⁵⁵ The CJEU has even required EU Member States to give Internet users judicial recourse in cases of OSP over-removal in some situations, saying that this correction mechanism is necessary to protect information access rights.²⁵⁶

252. *Id.* at 10.

253. *See, e.g.,* Erdos, *supra* note 137 (discussing ongoing dispute between Google and the Spanish DPA regarding webmaster notice). Interestingly, a Mexican court, applying data protection laws largely derived from Spain’s, concluded that notice to the webmaster was *mandatory* in order to protect the webmaster’s rights before the DPA could enforce a RTBF claim. Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región [TC], http://sise.cjf.gob.mx/SVP/word1.aspx?arch=1100/11000000188593240001001.docx_0&sec=_Mercedes_Santos_Gonz%C3%A1lez&svp=1 [https://perma.cc/6YW2-FBYN].

254. *See* Erdos, *supra* note 137.

255. *See supra* Section II.A.

256. Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2014 EUR-Lex CELEX LEXIS 62012CJ0314 ¶ 57 (Mar. 27, 2014) (holding that when courts order ISPs to block websites without specifying technical means of doing so, potentially leading to over-blocking of lawful information, “national procedural rules must provide a

Involving the content creator also opens up possibilities for better-tailored solutions to online privacy violations. OSPs typically face a binary choice—take information down or leave it up.²⁵⁷ But a content creator can do much better by rewording a phrase, updating or annotating a news story, or taking down one sentence of a blog post while leaving lawful text intact.²⁵⁸ Webmasters can also use technical tools to control whether search engines index their pages.²⁵⁹

Following the reasoning of the *Google Spain* guidelines, OSPs should contact publishers only in special cases, where their input is needed to resolve a removal request. In practice, such a limited exception only protects Internet users' rights if OSPs themselves accurately identify flawed notices and initiate individual communication about each one. That approach defeats a key purpose of notifying the affected publisher: correcting for errors made by the OSP itself. For example, if Twitter does not know that Matilda Humperdink's party was a fast-food restaurant opening, it may not recognize any public

possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known").

257. There are other logical possibilities, but most—like taking a scene out of a hosted video—would endanger the intermediary's protections under the eCommerce Directive or other intermediary liability laws. C-236/08, *Google France SARL v. Louis Vuitton Malletier SA*, 2010 E.C.R. I-02417, 02514 ¶ 120 (holding that OSPs which take too active a role regarding content may lose immunity).

258. These practical remedies are closely analogous to those sometimes offered by press archives, such as allowing annotation, rectification, or reply to inaccurate articles. *See, e.g.*, Anjuman Ali, *Corrections and Clarifications*, WASH. POST (Sept. 1, 2011), <http://www.washingtonpost.com/wp-srv/guidelines/corrections.html> [<https://perma.cc/3QJS-QASP>] (listing compilation of press best practices for updating and correcting stories without removing them).

259. Some authorities have, in the past, encouraged or required webmasters themselves to use technical tools to prevent indexation based on data protection obligations. *See, e.g.*, ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 227, at 58–59 (writing that news archives may balance data protection and free expression rights by using technical tools to block indexation); *cf.* Kuczerawy & Ausloos, *supra* note 5, at 229 (describing how a Belgian court ruled that publishers must sometimes prevent indexation); Aurelia Tamò & Damian George, *Oblivion, Erasure and Forgetting in the Digital Age*, 5 J. INTELL. PROP. INFO. TECH. & E-COM. L. 71, 81 & n.121–23 (2014) (explaining that the Italian DPA requires news archives to block indexation) (citing *Archivi Storici on Line dei Quotidiani: Accoglimento dell'Opposizione dell'Interessato alla Reperibilità delle Proprie Generalità Attraverso i Motori di Ricerca*, IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (Dec. 11, 2008), <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1583162> [<https://perma.cc/YV4L-5F4T>]). The Constitutional Court of Colombia reached a similar outcome in a post-*Google Spain* case assessing the RTBF under Colombia's data protection law. *See* “L,” a Nombre Suyo y de su Hijo “P,” Menor de Edad v. el Instituto Colombiano de Bienestar Familiar, Corte Constitucional [C.C.] [Constitutional Court], julio 15, 2013, Sentencia T-453/13 (Colom.), <http://www.corteconstitucional.gov.co/relatoria/2013/T-453-13.htm> [<http://perma.cc/8GL2-JQFX>].

interest in the tweet about her food making people sick. By contrast, if notice to accused speakers is a standard practice, and not an exceptional step instituted by the OSP, the opportunity for error-correction is put in the hands of the person best motivated and equipped to use it.

d) Telling the Public What Information Has Been Erased

The GDPR is silent on the question of transparency to the public about RTBF erasures, seeming to preserve the status quo from the 1995 Directive. This almost certainly means that OSPs can only be transparent in ways that do not identify the person who sought removal. After all, any disclosure that identified the data subject would itself likely constitute an unauthorized processing of personal information.²⁶⁰ This standard permits some established public transparency practices for notice-and-takedown but precludes important other ones.

Transparency reports consisting of aggregated figures—including the number of requests received, the number granted, how many came from which country—appear to be permitted under the GDPR.²⁶¹ Similarly, the GDPR does not preclude transparency about the rules an OSP applies in assessing requests, with the exception of rules so specific to an unusual case that they would effectively identify the requesting party.

But transparency about what information has been affected by removal requests is very difficult under the GDPR. Even disclosing a page URL or file name could effectively identify the person who objected to it. This is a problem for OSPs who might otherwise post an explanatory “tombstone” notice to users when content they seek has been removed—like the copyright removal notices on YouTube. This restriction on disclosing removal requests also harms OSPs’ ability to share copies of removal requests with public repositories like the Lumen database, operated by Harvard Law School’s Berkman Center. The Lumen database archives redacted copies of legal removal requests.²⁶² In addition to enabling significant scholarship, the database lets any interested party identify when content has been removed improperly.²⁶³ In conjunction with OSPs’ notices to users, the Lumen database

260. See GDPR, *supra* note 6, art. 6 (enumerating lawful bases for processing); 1995 Directive, *supra* note 69, art. 7 (same).

261. In 2018, Google published a report providing unprecedented quantitative information about resolution of RTBF requests. See BERTRAM ET AL., *supra* note 8.

262. See Lumen Database, *supra* note at 27.

263. See Brief of Amici Curiae, *supra* note 42, at 7, 21; Daphne Keller, Comment on the Guidelines on Transparency Under Regulation 2016/679 (Jan. 23, 2018), <http://cyberlaw.stanford.edu/files/publication/files/KellerA29GDPRTransparencyComments.pdf> [<https://perma.cc/CU5F-JLB5>] (discussing ways the Working Party or new Board could work with trusted researchers to increase transparency).

effectively crowdsources the job of error correction. This important check on over-removal will probably not be available for RTBF requests under the GDPR. It may be possible, though, for regulators to approve of more limited disclosure—perhaps to academic researchers—as permissible processing of personal data from RTBF requests.

The absence of more robust public transparency makes other procedural checks on over-removal, discussed throughout this Section and in Section II.A, all the more important.

D. FREE EXPRESSION AND INFORMATION PROTECTIONS

The other important GDPR provisions affecting RTBF requests come from the law's express provisions on information and expression rights. Unfortunately, those provisions are scant in both substance and procedural enforcement mechanisms.

1. *Express General Data Protection Regulation Provisions*

The GDPR lists “the right of freedom of expression and information” as a basis for OSPs to decline RTBF requests.²⁶⁴ However, as van Hoboken wrote of an earlier GDPR draft, “its lack of clarity about the scope and substance of exceptions and derogations to be made in view of freedom of expression raises very serious questions.”²⁶⁵ While the GDPR carefully details the data protection side of this balance, it leaves individual EU Member States to “reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information[.]”²⁶⁶

This is the same allocation of responsibility to Member States that exists under the current 1995 Directive, and empirical research reveals significant problems with it.²⁶⁷ Cambridge's David Erdos has exhaustively reviewed and analyzed national free expression carve-outs from data protection law and found significant and troubling variation from one country to another.²⁶⁸

264. GDPR, *supra* note 6, art. 17(3)(a).

265. VAN HOBOKEN, *supra* note 160, at 29.

266. GDPR, *supra* note 6, art. 85; *see also* Daphne Keller, *The GDPR and National Legislation: Relevant Articles for Private Platform Adjudication of “Right to Be Forgotten” Requests*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y (May 1, 2017, 2:57 PM) <http://cyberlaw.stanford.edu/blog/2017/05/gdpr-and-national-legislation-relevant-articles-private-platform-adjudication-%E2%80%9Cright-be> [<https://perma.cc/GKF5-NX9E>] (listing relevant GDPR articles for Member State implementation).

267. 1995 Directive, *supra* note 69, art. 9.

268. Erdos concludes that “many Member States have failed to provide for an effective balance [between] . . . media freedom . . . [and] data protection.” David Erdos, *European Union Data Protection Law & Media Expression: Fundamentally Off Balance*, 65 INT'L & COMP. L.Q. 139, 141 (2016).

Some countries have not even passed the free expression legislation mandated decades ago under the 1995 Directive.²⁶⁹ Others have enacted laws that fall far short of the goal of balancing expression and privacy rights. Given this history, it seems unrealistic to expect better outcomes under the GDPR.

Another problem is that while Article 85 of the GDPR specifically requires Member States to create exemptions for “journalistic . . . academic, artistic or literary expression,” legal protections are less clear for expression that does not fall in one of these four categories.²⁷⁰ That is a problem for OSPs struggling to interpret the law, because valuable online expression often falls outside of those four enumerated categories. A tweet about a dishonest car mechanic, a Yelp review of a botched medical procedure, or a post criticizing an individual Etsy or Amazon vendor may not be covered. Neither might a personal blog post recounting domestic abuse. This kind of material appears to be a far cry from the privileged—and often professionalized and even licensed—categories of expression listed in Article 85(2).²⁷¹ But it is precisely this democratic cacophony that makes the Internet so different from prior speech platforms. Without clear free expression protections to guide OSPs, this speech is at risk.

Also troubling is the GDPR’s lack of clarity about *whose* free expression rights an OSP should consider. The most obvious person should be the

269. *Id.* at 151 (“The laws of three countries (Croatia, Czech Republic and Spain) provide no media derogation at all from any part of the data protection scheme.”) (internal citations omitted).

270. GDPR, *supra* note 6, art. 85. For the four enumerated categories of expression, the GDPR requires that Member States “shall provide for exemptions or derogations” and notify the Commission of “the provisions of its law which it has adopted”—suggesting countries must enact written laws on point. *See id.* art. 85(2)–(3). For other kinds of free expression, Member States need only “by law reconcile” the rights, which might just mean requiring judges to consider them. *Id.* art. 85(1); *see also* David Erdos, *From the Scylla of Restriction to the Charybdis of License? Exploring the Present and Future Scope of the “Special Purposes” Freedom of Expression Shield in European Data Protection*, 52 COMMON MKT. L. REV. 119, 128–41 (2015) (exploring tensions between the special-purpose free-expression provisions in the GDPR and its data protection provisions).

271. *See* VAN HOBOKEN, *supra* note 160, at 23 (discussing role of “doctrines that were traditionally reserved for the institutionalized press” in context of blogs and other non-professionalized expression); Case C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy*, 2008 E.C.R. I-09831, ¶¶ 56–62 (applying journalism exemptions broadly to “disclosure to the public of information, opinions or ideas”). A case referred to the CJEU in 2017 asks whether a user who uploaded police footage to YouTube can claim the journalism exemption. Case C-345/17, *Sergejs Buivids v. Datu Valsts Inspekcija*, 2017 EUR-Lex CELEX LEXIS 62017CN0345 (June 12, 2017) (“Do activities such as those at issue in the present case, that is to say, the recording, in a police station, of police officers carrying out procedural measures and publication of the video on the Internet site www.youtube.com, fall within the scope of Directive 95/46?”).

publisher or Internet user who posted the content. But in real-world litigation, serious legal uncertainty can arise regarding an intermediary's ability to act on the basis of that user's rights—as opposed to the company's own, relatively paltry, free expression rights. As a conspicuous example, the CJEU's *Google Spain* ruling itself did not identify the publisher's expression rights as a balancing factor that Google should consider in removing search results.²⁷² Even the ECHR, in one intermediary liability case, appeared to base its analysis on the rights of the OSP—though in a later case it shifted focus to the platform's users.²⁷³ Internet users' rights should be a central concern of notice-and-takedown systems, and OSPs, regulators, and courts should expressly take them into consideration.

Data protection law's lack of detailed provisions for free expression made sense in an era when regulated data consisted of records held by banks, employers, medical offices, and the like. With data protection emerging as a major law governing users' speech on Internet platforms, however, uncertainty about these protections will chill legitimate online expression. The law's own inadequacies will ramify as it is interpreted by risk-averse private companies under the GDPR's notice-and-takedown framework. Unfortunately, as will be discussed in the next Section, public adjudication and regulatory review are unlikely to correct this imbalance.

2. Enforcement Processes

The processes for courts and regulators to resolve disputes involving privacy and free expression under the GDPR are significantly unbalanced.²⁷⁴ A person asserting a privacy or data protection right has state support and a

272. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317, ¶ 97.

273. Compare *Delfi AS v. Estonia*, App. No. 64569/09, Eur. Ct. H.R. 586, ¶¶ 140, 162 (2015) (considering the rights of platforms), with *Magyar Tartalomszolgáltatók Egyesülete (MTE) v. Hungary*, App. No. 22947/13, Eur. Ct. H.R. 135 ¶¶ 36–39, 61, 82, 86, 88 (2016) (considering the rights of Internet users); see also Daphne Keller, *Litigating Platform Liability in Europe: New Human Rights Case Law in the Real World*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y (Apr. 13, 2016, 5:00 AM), <http://cyberlaw.stanford.edu/blog/2016/04/litigating-platform-liability-europe-new-human-rights-case-law-real-world> [<https://perma.cc/38X7-6LZV>].

274. The ECHR has spoken to the importance of judicial review to avoid over-removal of lawful online content. *Yildirim v. Turkey*, App. No. 3111/10, Eur. Ct. H.R. ¶ 68 (2012) (holding that site blocking violates Convention rights where “the judicial review procedures concerning the blocking of Internet sites are insufficient to meet the criteria for avoiding abuse, as domestic law does not provide for any safeguards to ensure that a blocking order in respect of a specific site is not used as a means of blocking access in general.”); see also Case C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*, 2014 EUR-Lex CELEX LEXIS 62012CJ0314 ¶ 57 (Mar. 27, 2014).

clear avenue to enforce those rights. A person asserting a countervailing free expression right does not. In this respect, public adjudication by DPAs and courts has many of the same systemic imbalances as the GDPR's private notice-and-takedown process.

The basic sequence of events is as follows. When an OSP does not comply with a RTBF removal request, the requester can take her grievance to the regional or national DPA.²⁷⁵ For example, if Twitter declines to remove the Matilda tweet and Matilda lives in Sweden, she could complain to the DPA there. The DPA adjudicates the matter as a two-party dispute between the data subject (Matilda) and the OSP (Twitter), typically under strict rules of confidentiality.²⁷⁶ The person whose free expression rights are at stake, the author of the tweet in this case, is typically absent from the process.²⁷⁷ The unknown Internet users and potential restaurant diners who might benefit from reading the tweet are of course also absent. Defending their rights before the DPA falls to the OSP, which likely does not know if the review is telling the truth and has little incentive to litigate on the user's behalf.

DPAs' mandates nominally extend beyond data protection: they are "to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union."²⁷⁸ In practice, DPAs have shown real sensitivity to free expression concerns, including in the thoughtful RTBF public interest criteria released by the Article 29 Working Party.²⁷⁹ But DPAs remain, in most cases, bodies of privacy professionals (not necessarily lawyers)²⁸⁰ whose job is to regulate the

275. GDPR, *supra* note 6, art. 77. GDPR Article 79 also allows data subjects to go directly to a court. *Id.* art. 79.

276. *Id.* art. 54(2).

277. See ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 10. There is an interesting question about what happens if an intermediary has accepted the Article 29 Working Party's authorization to contact the affected speaker in particularly difficult removal cases. Can that person then be included in any subsequent procedure before a DPA or courts? The GDPR does interestingly provide that "each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them." GDPR, *supra* note 6, art. 78(1). Arguably, this should open the door for an affected speaker to get into court once a DPA orders an OSP to delete her speech, even if she was not a party before the DPA.

278. GDPR, *supra* note 6, art. 51(1). Note that this mandate is broader than the one DPAs held under the 1995 Directive. See 1995 Directive, *supra* note 69, art. 28.

279. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 103, at 12–20.

280. See INT'L ASS'N OF PRIVACY PROF'LS, DATA PROTECTION AUTHORITIES: 2011 GLOBAL SURVEY 14 (2011), https://iapp.org/media/pdf/knowledge_center/DPA11_Survey_final.pdf [<https://perma.cc/8T6X-TZK2>] ("DPA offices employ staff with a wide variety of advanced degrees, the most prevalent areas being computer science and business administration . . .").

processing of personal data. Absent a far stronger legal mandate for them to balance privacy with free expression, and without including free expression experts as important actors within the agencies, it is not reasonable to expect DPAs to be equally attuned to both sets of rights. This natural focus on the privacy side of the equation can only be amplified when the person asserting a privacy harm stands before them, while the people who might suffer information harms are nowhere to be seen.

The only regulatory review under pre-GDPR data protection law of a rejected RTBF was typically before a national DPA.²⁸¹ At that point either the data subject or the OSP could move the dispute to national court.²⁸² The GDPR changes this by adding another potential level of regulatory review by the new EU Data Protection Board.²⁸³ The Board will review cases and issue opinions to harmonize differences between national DPAs—differences which, in the free expression context, may easily arise from divergent Member State law. For example, the Swedish DPA might agree with Twitter that the public has an interest in knowing about dangerous food. But if a factually similar case arose in Estonia, that DPA might think Matilda’s data protection interests are stronger.²⁸⁴ When the Board reviews such a dispute, just as when a DPA does, there is no apparent notice to or role for the Internet user whose online speech is being assessed.

Oddly, one GDPR Recital suggests that Member State courts may not review Board decisions, including those balancing free expression and privacy rights:

[W]here a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board’s decision invalid but must refer the question of validity to the Court of Justice²⁸⁵

So, if the Swedish and Estonian DPAs disagreed about Matilda’s complaint or about the principles governing complaints of that type, the Board could potentially resolve the issue. One or both national DPAs would then resolve

281. 1995 Directive, *supra* note 69, art. 22 (providing judicial remedies); *Id.* art. 28(4) (providing administrative remedies).

282. *Id.* art. 28(3).

283. GDPR, *supra* note 6, art. 65.

284. The GDPR’s provisions to coordinate among national DPAs are unlikely to resolve this issue or reach a harmonized outcome, because doing so would effectively nullify Article 85’s reservation of power to Member States to set their own free expression laws. *See supra* Section III.E.

285. GDPR, *supra* note 6, recital 143.

disputes or issue orders on the basis of the Board's decision. A Swedish court reviewing those orders would seemingly not be permitted to nullify the Board's decision, even if it conflicted with Swedish free expression law as interpreted by the court. Following this strange avenue, a dispute about the balance between data protection and information rights could in theory make it all the way to the EU's highest court without the core information rights issue ever being resolved by a judge in a Member State. This avenue would make sense if the GDPR were a purely harmonized, EU-wide legal framework. But it is not: the GDPR expressly leaves free expression protections to Member States, preserving national differences in this area of law.²⁸⁶ That makes the potential exclusion of Member State courts from the data protection versus free expression balancing exercise very troubling.²⁸⁷ A dispute that made its way to the CJEU by this means would also apparently exclude the affected original publisher. As in the *Google Spain* case, the court would hear argument from the OSP only.²⁸⁸

By contrast to this multi-stage process for a claimant raising a privacy right, the legal path for a claimant raising a free expression right under the RTBF is short and disappointing. Regulatory review is typically not an option.²⁸⁹ No publicly funded, legally powerful "Information Rights Agency" stands as an institutional counterweight to DPAs. In most cases, an Internet user or publisher's only recourse is to courts of law, where she can attempt to sue either the OSP or the data subject who requested removal. Neither claim is likely to succeed. Legal claims against OSPs for "wrongful removal" have historically failed, even in cases where OSPs deleted user speech based on their own discretionary content guidelines.²⁹⁰ Such claims are even less likely to

286. *Id.* art. 85.

287. One alternate interpretation of the provision is that national courts can require national DPAs to not comply with Board decisions, but cannot overrule the Board itself. Another is that the national court could consider the case, but only after a CJEU referral. Either interpretation seems odd.

288. La Vanguardia was initially a party to *Google Spain*, but ceased to be when the Spanish DPA determined that its processing was lawful. Peguera, *supra* note 5, at 524.

289. The GDPR requires DPA review only for claims based on data protection rights. *See* GDPR, *supra* note 6, art. 57(1)(f).

290. In the United States, multiple "wrongful removal" claims have been rejected by courts. *See, e.g.,* Lewis v. YouTube, LLC, 244 Cal. App. 4th 118 (Cal. Ct. App. 2015); Darnaa, LLC v. Google, Inc., No. 15-cv-03221-RMW, 2015 WL 7753406 (N.D. Cal. Dec. 2, 2015); Song Fi Inc. v. Google, Inc., 108 F. Supp. 3d 876 (N.D. Cal. 2015). In a high profile case brought against Facebook for removing a famous painting under its nudity policy, a French court ruled that the social network violated its contractual obligations by terminating the plaintiff's account without prior notice, but did not order the image reinstated or award damages. Philippe Sotto, *French Court Issues Mixed Ruling in Facebook Nudity Case*, AP NEWS

succeed when, as with RTBF removals, an OSP erases expression based on a perceived legal obligation.²⁹¹ And there is typically no clear cause of action against an individual whose claim led an OSP to remove content.²⁹² Publishers, speakers, and Internet users deprived of access to information under the GDPR may have no remedy.

E. JURISDICTION

A final threat to free expression rights comes from the GDPR's extraterritoriality provisions.²⁹³ These are deliberately expansive, applying EU

(Mar. 15, 2018), <https://www.apnews.com/ebbd9a846504460ea184201dcce303d> [<https://perma.cc/N36V-JR9B>].

291. The issue of user rights and remedies for “wrongful removal” is a fruitful area for further scholarship and is increasingly discussed in the human rights literature. *See, e.g.*, David Kaye, *Rep. of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶¶ 52, 67–71, U.N. Doc. A/HRC/32/38 (May 11, 2016), <https://undocs.org/A/HRC/32/38> [<https://perma.cc/FFK3-N27J>]; KORFF, *supra* note 21. However, this author has found no published legal analysis about black-letter law, doctrinal bases for such claims against OSPs. One possible argument comes from the CJEU's *Telekabel* ruling, which allowed Internet users to contest over-removal resulting from a court order. *See* Case C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*, 2014 EUR-Lex CELEX LEXIS 62012CJ0314 ¶ 57 (Mar. 27, 2014). By analogy, arguably users should be able to contest other legally motivated over-removals. But such an argument could easily fail because the role of state action in ordinary notice-and-takedown claims from private parties, such as RTBF claims, is attenuated in comparison to the state action of the court order in *Telekabel*. *See id.*

292. Assuming that an affected speaker found out about the RTBF removal and could identify the wrongful accuser, the speaker could in theory sue based on a tort theory. *See, e.g.*, BRITISH INST. OF INT'L & COMPARATIVE LAW, INTRODUCTION TO FRENCH TORT LAW, www.biicl.org/files/730_introduction_to_french_tort_law.pdf [<http://perma.cc/RG9N-DWHR>] (listing elements of French tort claim); JUDICIAL COUNCIL OF CAL., 2202. *Intentional Interference with Prospective Economic Relations—Essential Factual Elements*, in JUDICIAL COUNCIL OF CALIFORNIA CIVIL JURY INSTRUCTIONS 1247 (2018), http://www.courts.ca.gov/partners/documents/caci_2018_edition.pdf [<https://perma.cc/5ZL8-TVJF>]; Code civil [C. civ.] [Civil Code] art. 1382–84 (Fr.) (general tort claim). However, the loss of indexation or hosting services is unlikely to constitute sufficient damage to support such a claim. *See id.* This author's research has identified no cases attempting to raise such arguments in the EU. In the RTBF context, the Spanish DPA has suggested that webmasters affected by delisting do not even have an affected legitimate interest because “search engines do not recognize a legal right of publishers to have their contents indexed.” Erdos, *supra* note 137. The DPA's analysis is flawed because it conflates speakers' rights against private action with their rights against state action or state-mandated action. But it is indicative of the barriers that a claimant would face.

293. Territorial application of EU data protection law is complex and largely beyond the scope of this Article. Because extraterritorial application of the 1995 Directive was disputed, some practitioners may argue that EU data protection law always applied as broadly as it does under the GDPR. The issue is well examined in Michel Jose Reymond, *Hammering Square Pegs into Round Holes: The Geographical Scope of Application of the EU Right to Be Delisted* (Berkman Klein Ctr. for Internet & Soc'y at Harvard Univ., Research Publication No. 2016-12, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838872 [<https://perma.cc/DWD2->

data protection law to many foreign actors in an effort to protect European privacy rights more effectively. To the extent the GDPR leads to unintended harms to the information and privacy rights of people who post content online, that harm will be exported through application of EU or Member State law to information shared in other countries.

1. *Prescriptive Jurisdiction: Who Must Comply?*

The GDPR expands the reach of EU data protection law in several ways.²⁹⁴ Most importantly, it covers entities outside the EU if they process personal data of EU users in relation to the “monitoring of their behaviour.”²⁹⁵

“Monitoring” is not defined in the GDPR, but a Recital explains that it includes tracking a data subject for purposes of “profiling,” including “predicting her or his personal preferences.”²⁹⁶ “Profiling” is defined, and very broadly. It means:

[A]ny form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements²⁹⁷

This definition would appear to cover standard online customization, like the articles recommendations for individual users in the New York Times online, as well as individually targeted advertising. For the untold number of entities with features like these, serving EU users will likely mean falling under the GDPR.²⁹⁸ The extraterritorial effect is still greater if “monitoring” covers standard web analytics programs that track IP addresses of users.

HX9S] and Brendan van Alsenoy & Marieke Koekoek, *Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the “Right to Be Delisted”*, 5 INT’L DATA PRIVACY L. 105 (2015).

294. GDPR, *supra* note 6, art. 3(2).

295. *Id.* art. 3(2)(b). Another new provision applies the GDPR to entities engaged in “the offering of goods or services . . . [to] data subjects in the Union” *Id.* art. 3(2)(a). This basis for jurisdiction is relatively cabined by a Recital explaining that mere accessibility of a site to EU users does not establish jurisdiction, and that factors like the language of the site or the currency used for transactions should be considered. *Id.* recital 21; *see also* Michel Reymond, *Jurisdiction in Case of Personality Torts Committed over the Internet: A Proposal for a Targeting Test*, 14 Y.B. PRIV. INT’L L. 205, 205 (2013) (discussing “targeting” jurisdiction analysis in the EU).

296. GDPR, *supra* note 6, recital 24.

297. *Id.* art. 4(4).

298. There is room for argument that jurisdiction does not attach unless an OSP intended to monitor EU users. *See* Case C-101/01, *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, 2003 E.C.R. I-12976, 13017 ¶¶ 59–60 (applying an intent standard for data transfer provisions

Where does all this really leave non-EU companies that do business online? For large companies that already offer services to European markets and have invested in compliance with current data protection law, the transition will take work but should not pose insurmountable difficulties. For smaller companies that have never operated in the EU but have some users there, the picture is very different. Some reacted to the GDPR's passage by blocking European users, rather than taking on compliance costs.²⁹⁹ Realistically, the GDPR may never actually be enforced against them. On the other hand, complaints from disgruntled users, whether valid or invalid, could at any time bring regulatory attention to obscure or distant entities. Thus, both uncertainty and actual or perceived financial exposure under the GDPR are high.

2. *Territorial Scope of Compliance: Must OSPs Erase Content Globally?*

Once an entity is subject to RTBF obligations under the GDPR, must it comply globally by erasing content for users all over the world—even in countries where the material is legal? The GDPR does not directly address this question, and neither did the *Google Spain* ruling. As this Article went to press, however, the CJEU was preparing to review a case in which the French DPA ordered Google to delist search results globally.³⁰⁰ Google has so far limited its compliance to services targeted to or available in Europe, and argued that people in other countries have the right to access the delisted information

under the 1995 Directive). Once an EU user communicates a RTBF request to an OSP, though, it arguably knows of and intends to monitor that user.

299. Rebecca Hill, *US Websites Block Netizens in Europe: Why Are They Ghosting EU? It's Not You, It's GDPR*, REGISTER (May 25, 2018, 9:06 AM), https://www.theregister.co.uk/2018/05/25/tronc_chicago_tribune_la_times_gdpr_lock_out_eu_users/ [https://perma.cc/L6LR-CUDN]; James Sanders, *To Save Thousands on GDPR Compliance, Some Companies Are Blocking All EU Users*, TECHREPUBLIC (May 7, 2018, 6:50 AM), <https://www.techrepublic.com/article/to-save-thousands-on-gdpr-compliance-some-companies-are-blocking-all-eu-users/> [https://perma.cc/CA6R-WS56].

300. Press Release, *supra* note 135; Commission Nationale de l'Informatique et des Libertés, *supra* note 135.

under their own national law.³⁰¹ Resolution of this case will likely shape outcomes under the GDPR—including outcomes for hosts and other OSPs.³⁰²

This is not solely a matter of conflict between EU and non-EU law. The same questions arise when law varies between EU Member States, as it inevitably will. The GDPR, like the 1995 Directive, expressly contemplates that laws balancing data protection with free expression will not be harmonized, but will be unique to each Member State.³⁰³ Current divergence between national laws will persist under the GDPR.³⁰⁴ It is entirely foreseeable that, as described in the example of the Matilda tweet, one nation might require an OSP to remove a link or content, while another does not. Which country's law should prevail? The GDPR says it should be “the law of the Member State to which the controller is subject,” but for non-EU companies with operations throughout the EU, this is unlikely to resolve the problem.³⁰⁵

As with so many unanswered questions under the GDPR, this one creates systematic pressure in favor of more content removal. If RTBF removals must be global and Estonian and Swedish laws conflict, an OSP could face fines in Estonia for failing to remove content in Sweden. By contrast, Swedish regulators are unlikely to notice or react if the OSP removes the content in order to avoid legal trouble in Estonia. If this dynamic persists, national law

301. Kent Walker, *A Principle That Should Not Be Forgotten*, GOOGLE EUR. (May 19, 2016), <https://www.blog.google/topics/google-europe/a-principle-that-should-not-be-forgotten/> [<https://perma.cc/8837-ABLX>]. Google initially carried out RTBF removals on country-targeted versions of its search service, which operated on national domains such as google.fr. In 2016 it changed approach, using technical tools to block access to delisted results based on the user's estimated geographic location. Peter Fleischer, *Adapting Our Approach to the European Right to Be Forgotten*, GOOGLE EUR. (Mar. 4, 2016), <https://www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig/> [<http://perma.cc/W4L9-HNBX>]. In 2017, the company shifted to providing nationally-targeted versions of web search based on entirely users' location and settings, regardless of the national domain in the URL. Evelyn Kao, *Making Search Results More Local and Relevant*, KEYWORD (Oct. 27, 2017), <https://www.blog.google/products/search/making-search-results-more-local-and-relevant/> [<https://perma.cc/ECH2-7UCM>].

302. See Case C-507/17, *Google Inc. v. Commission Nationale de l'Informatique et des Libertés*, 2017 EUR-Lex CELEX LEXIS 62017CN0507 (Aug. 21, 2017), https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.C_.2017.347.01.0022.02.ENG [<https://perma.cc/HY2H-J8EM>].

303. GDPR, *supra* note 6, art. 85; see also *supra* Section III.D. Member State law differences of this sort, which arise from differing Member State free expression rules, are unlikely to be resolved by the GDPR's consistency mechanism for reconciling differences of data protection law interpretation among DPAs. GDPR, *supra* note 6, art. 64(1).

304. See Erdos, *supra* note 268, at 146–49 (identifying wide variation in national law balancing data protection and free expression rights).

305. GDPR, *supra* note 6, recital 153.

favoring deletion can be expected to consistently displace other countries' laws favoring user expression.

IV. RELATION TO NOTICE-AND-TAKEDOWN RULES OF THE ECOMMERCE DIRECTIVE

Internet users and OSPs could be spared the GDPR's problematic takedown rules through a seemingly simple legal move: applying the EU's existing intermediary liability laws under the eCommerce Directive. This Article uses the term "eCommerce Rules" to refer to the procedural rules derived from the Directive itself, Member States' implementing legislation, and interpretations in case law. These rules provide far more balanced protections than the confusing "GDPR Rules" discussed in Part III. Importantly, a key GDPR provision suggests that the GDPR's drafters actually intended to invoke and apply the eCommerce Directive.³⁰⁶ If this is the case and eCommerce Rules *do* cover RTBF removals, then many of the problems this Article has identified with the GDPR Rules are solved. The GDPR Rules would remain effective and meaningful, but would apply only to erasure of stored back-end data, such as logs or profiles.

Unfortunately, as will be discussed in this Part, doctrinal conflicts could prevent this outcome. The law on point is messy, with arguments on both sides. As with so many of the GDPR's ambiguities, this one creates bad incentives for OSPs to play it safe and accept the interpretations that most favor removal—and that least protect other Internet users' rights.

A. PROCEDURAL PROTECTIONS FOR INFORMATION RIGHTS UNDER THE ECOMMERCE DIRECTIVE

There are a number of good reasons to apply eCommerce Rules to RTBF notice-and-takedown. One reason is for consistency and fairness among people seeking content removal. The GDPR alone would give RTBF claimants a procedural shortcut compared to those alleging defamation, non-data protection privacy torts, and other harms—all of whom must clear the procedural hurdles of the eCommerce Directive. Nothing about RTBF claims justifies this leg up over other long-established claims, including conventional civil privacy claims. The procedural advantage, combined with the ease of prevailing on RTBF requests as a substantive matter, encourages gaming the system of removal claims and litigation.³⁰⁷ Indeed, in the wake of the *Google*

306. *Id.* art. 2(4); *see also infra* Section IV.B.2.b.

307. *See, e.g.,* Ashley Hurst, *Data Privacy and Intermediary Liability: Striking a Balance Between Privacy, Reputation, Innovation and Freedom of Expression, Part 1*, INFORRM'S BLOG (May 14, 2015), <https://inforrm.wordpress.com/2015/05/14/data-privacy-and-intermediary-liability->

Spain case, many individuals who had previously alleged defamation or other harms refiled removal requests and complaints under new RTBF theories.³⁰⁸

More fundamentally, the eCommerce Rules do a better job of balancing the rights of all parties who are affected by notice-and-takedown—including Internet users whose free expression and information rights are affected. They do so through two key standards. First, the eCommerce “knowledge” standard for OSPs means that OSPs do not have to remove user expression based on inadequately substantiated allegations.³⁰⁹ By contrast, the GDPR’s “restriction” rule encourages or requires OSPs to do exactly that—to remove first, and ask questions later.³¹⁰ Second, the eCommerce rule against making OSPs pervasively monitor users’ communications is an important protection for user rights. If platforms did have to police online speech, they would be strongly motivated to err on the side of over-removal or to simply not offer open public access to platforms. Courts including the CJEU and ECHR have recognized the threat this poses to information and expression rights, and the CJEU has noted that such monitoring also threatens user privacy rights.³¹¹ The Directive also encourages Member States to enact additional procedural protections, as some have done.³¹² By contrast, diverging national notice-and-takedown rules would arguably conflict with the GDPR’s harmonization goal.³¹³

Of course, the eCommerce Directive has problems of its own. Its provisions are inconsistently applied across the EU, it has too often been interpreted in ways that erode its free expression protections, and it is under

striking-a-balance-between-privacy-reputation-innovation-and-freedom-of-expression-part-1-ashley-hurst/ [http://perma.cc/VBW6-JH99] (noting that using data protection claims in lieu of privacy or defamation gives plaintiffs “a potential short cut” and avoids “lengthy debate about such terms as ‘reasonable expectation of privacy’ . . .”).

308. This is based in part on the author’s personal knowledge. *See also* Hurst, *supra* note 307 (identifying RTBF claims as a shortcut for defamation claimants). In *NT 1 and NT 2*, a British court rejected Google’s argument that RTBF claimants were abusing legal process by circumventing the restrictions of defamation law. *NT 1 & NT 2 v. Google*, [2018] EWHC 799 (QB). By contrast, in a pre-*Google Spain* case, a British court held that data protection law did not “afford a set of parallel remedies when damaging information has been published about someone, but which is neither defamatory nor malicious,” and noted its presumption that a plaintiff relying on a data protection claim did so because he could not succeed on a defamation claim. *Quinton v. Peirce* [2009] EWHC 912 (QB), ¶¶ 3, 87.

309. *See* Case C-324/09, *L’Oréal SA v. eBay Int’l AG*, 2011 E.C.R. I-6011, ¶ 22.

310. *Compare supra* Section II.A (eCommerce “knowledge” standard), *with supra* Section III.C.I.I.A.2 (GDPR “restriction” standard); *see also* Kuczerawy & Ausloos, *supra* note 5, at 241–43 (discussing the “manifestly illegal” standard from eCommerce discussions).

311. *See supra* note 62 and accompanying text.

312. *Mylly & Mylly*, *supra* note 54, at 226.

313. Member States could arguably still enact procedural rules as part of their free expression protections. *See* GDPR, *supra* note 6, art. 85.

serious political attack.³¹⁴ But the Directive remains, for now, the EU's core intermediary liability law and, as a result, there are real, sustained efforts underway to protect free expression online and preserve reasonable rules based on its provisions.³¹⁵ If the eCommerce Directive does not apply to Internet users who are targeted by bad-faith or groundless RTBF requests, the legal gains made through this advocacy and scholarship will not benefit them.

In principle, it would be possible to construct a sui generis, rights-respecting notice-and-takedown framework based strictly on fundamental rights, without relying on provisions of the eCommerce Directive. If lawmakers conclude that the Directive does not apply to RTBF notice-and-takedown, this is what they will have to do. A few rare cases provide guidance for such an undertaking.³¹⁶ ECHR precedent, for example, has limited OSP monitoring obligations based purely on human rights under the Convention.³¹⁷ But far more common are cases that merge statutory or Directive-level law with human rights, usually by interpreting intermediary liability laws in light of

314. See generally Keller, *supra* note 61.

315. See, e.g., Letter from Sophie Stalla-Bourdillon et al., Assoc. Professor in IT Law, Univ. of Southampton, to the European Comm'n, Open Letter to the European Commission - On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society (Sept. 30, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2850483 [<http://perma.cc/KZ62-VJKS>]; EUROPEAN DIG. RIGHTS, DECONSTRUCTING THE ARTICLE 13 OF THE COPYRIGHT PROPOSAL OF THE EUROPEAN COMMISSION (2d rev.), https://edri.org/files/copyright/copyright_proposal_article13.pdf [<http://perma.cc/9HMZ-FPH5>]; Christina Angelopoulos, *EU Copyright Reform: Outside the Safe Harbours, Intermediary Liability Capsizes into Incoherence*, KLUWER COPYRIGHT BLOG (Oct. 6, 2016), <http://kluwercopyrightblog.com/2016/10/06/eu-copyright-reform-outside-safe-harbours-intermediary-liability-capsizes-incoherence/> [<http://perma.cc/N8WP-QZEJ>]; ARTICLE 19, *supra* note 56.

316. Magyar Tartalomszolgáltatók Egyesülete (MTE) v. Hungary, App. No. 22947/13, Eur. Ct. H.R. 135 (2016); Delfi AS v. Estonia, App. No. 64569/09, Eur. Ct. H.R. 586, ¶¶ 44, 47 (2015) (assessing OSP monitoring requirements under human rights standards). ANGELOPOULOS ET AL., *supra* note 21, at 28, argue that CJEU case law also supports the proposition that, “even absent Article 15, [OSP monitoring obligations] would also be illegal under the EU’s fundamental rights framework.” (discussing *Netlog*, 2 C.M.L.R. 18) There is also considerable “soft law” material from human rights institutions. See, e.g., Frank LaRue et al., *Joint Declaration on Freedom of Expression and the Internet*, ORG. FOR SECURITY & COOPERATION EUR. (June 1, 2011), <https://www.osce.org/fom/78309?download=true> [<https://perma.cc/QH7W-26DD>]; Frank La Rue (Special Rapporteur), Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* at 12 ¶ 42, U.N. Doc. A/HRC/17/27 (May 16, 2011), http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [<https://perma.cc/R7XB-8HKK>].

317. See Magyar Tartalomszolgáltatók Egyesülete (MTE), App. No. 22947/13, Eur. Ct. H.R. ¶¶ 88–91 (rejecting monitoring obligation as inconsistent with rights under the European Convention for the Protection of Human Rights and Fundamental Freedoms).

fundamental rights.³¹⁸ If the eCommerce Directive does not apply to RTBF removals, this case law will have only limited value.

B. APPLICABILITY OF THE ECOMMERCE DIRECTIVE TO RTBF
REMOVALS

Until quite recently, collisions between the eCommerce Directive and data protection law were rare. As a result, few cases have attempted to reconcile the two. This Section reviews legal issues—some conceptual and some arising from language in governing legal instruments—that make such reconciliation complex. These questions will be particularly important if the problems with the GDPR’s notice-and-takedown process are resolved through litigation, rather than through regulatory or Member State lawmaker action.

1. *Conceptual Tensions Between Intermediary Liability and Data Protection*

There is a fundamental question about whether eCommerce Rules should, as a matter of principle, apply to the RTBF. The answer depends in part on how the purpose and function of intermediary liability is understood.

From one perspective, the RTBF looks like a textbook intermediary liability law. It tells OSPs when they need to remove content created by users. The legal obligation is content-based—it depends on what the user is saying. And the consequences for the affected users are the same as in any notice-and-takedown system: the ability to participate and seek or share information over the Internet is curtailed.

From another perspective, intermediary liability is irrelevant. As framed by data protection law, RTBF requests are not about holding OSPs liable for user-generated content.³¹⁹ The duty to erase arises from the controller’s own independent legal obligations—not from those of its users.³²⁰ Data protection

318. *See, e.g.*, Case C-70/10, *Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM)*, 2011 E.C.R. I-12006 (interpreting eCommerce Directive Article 15 in light of fundamental rights); Case C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*, 2014 EUR-Lex CELEX LEXIS 62012CJ0314 (Mar. 27, 2014) (interpreting a national order for ISP to block a website under copyright law and Directive 2001/29/EC in light of fundamental rights).

319. *See* Kuczerawy & Ausloos, *supra* note 5, at 7 (“[T]he ruling does not impose search engine liability over the publication of the original content. Instead, the scope of application is concentrated on the search engine’s activity of linking a specific search term (such as the name of an individual) with a specific search result. This operation, after all, is entirely controlled by the search engine.”)

320. By this reasoning, the eCommerce Directive arguably would also not protect OSPs from direct copyright or defamation liability for user content—only from secondary liability. This would seem to defeat the purpose of the Directive’s safe harbors, rendering OSPs liable for content they knew nothing about. *See* Opinion of Advocate General Szpunar, Case C-484/14, *McFadden v. Sony Music Entm’t Ger. GmbH*, 2016 E.C.R. 170, ¶ 64 (explaining that

law may oblige an OSP to suspend its *own* processing activities, even if those who posted the content acted lawfully, as happened with the news site in *Google Spain*.³²¹

It is also debatable whether RTBF obligations should be considered a form of “liability” under European standards at all. The GDPR refers separately to controllers’ “responsibilities” and “liabilities,” and seems to class RTBF obligations as the former.³²² This is consistent with the general legal framing of data protection compliance as an obligation or condition of doing business. Responsibility to honor erasure requests in principle exists independently of any liability in the sense of exposure to civil tort claims³²³ or monetary damages.³²⁴ Compliance can be seen as a condition of doing business, much as obtaining licenses might be a condition of doing business for a restaurant. If the eCommerce intermediary liability framework did not apply to legal obligations of this sort, then it might be inapplicable to the RTBF.

But applicability of the eCommerce Rules does not depend on the doctrinal basis of an OSP’s removal obligations. The Rules are relevant for any claim that holds OSPs legally responsible for information posted by a user. They apply, as Advocate General Szpunar has said, to “all forms of liability for unlawful acts of any kind, and thus to liability under criminal law, administrative law and civil law, and also to direct liability and secondary liability for acts committed by third parties.”³²⁵ The eCommerce Rules address both monetary damages and injunctive relief, prohibiting the former and limiting the scope of the latter.³²⁶ The Rules even apply to and limit the

the eCommerce Directive shields OSPs from “direct liability and secondary liability for acts committed by third parties”).

321. See Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317, ¶¶ 82–88.

322. GDPR, *supra* note 6, recitals 74, 79, 80.

323. See ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 95, at 13 (noting that search engine controller status for processing website content is “separate from the issue of liability for such processing”).

324. The GDPR generally uses the term “liability” in reference to financial damages to data subjects. See, e.g., GDPR, *supra* note 6, recitals 74, 146 (describing allocation of liability between processors and controllers); *id.* art. 47(2)(f) (same); *id.* art. 82 (creating a “[r]ight to compensation and liability” which provides damages to individuals harmed by data processing).

325. Opinion of Advocate General Szpunar, Case C-484/14, *McFadden v. Sony Music Entm’t Ger. GmbH*, 2016 E.C.R. 170, ¶ 64.

326. eCommerce Directive, *supra* note 12, art. 15; Case C-70/10, *Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM)*, 2011 E.C.R. I-12006 (rejecting over-broad injunctions under Article 15). The eCommerce immunity provisions also address liability beyond monetary damages. See eCommerce Directive, *supra* note 12, art. 14(1)(a) (distinguishing constructive knowledge standard for damages from actual knowledge

obligations that may be placed on OSPs in cases where an OSP has no formal “liability” but is nonetheless obliged to take action under the law of a Member State.³²⁷ So, for purposes of determining whether eCommerce Rules apply to the RTBF, it does not matter whether RTBF obligations are considered a form of liability or are rooted in some other legal doctrine.

From the perspective of fundamental rights, these questions are largely semantic. A person whose expression is erased or delisted suffers the same harm—and state action plays the same role in creating that harm—regardless of what law prompted the OSP’s action. What matters to the affected users is that private companies, operating under actual or perceived legal compulsion, erased their expression—and did so without giving notice or providing an opportunity to object to the erasure. The procedural protections of intermediary liability law exist to address this problem.

2. *Confusing Language in the Governing Instruments*

Uncertainty about whether eCommerce Rules should apply to the RTBF as a principled matter is compounded by unclear prescriptions in the written law. The GDPR has language that might or might not resolve the entire issue by expressly invoking the eCommerce Rules for RTBF notice-and-takedown. Meanwhile, the eCommerce Directive contains language that might or might not prevent eCommerce Rules from applying to data protection claims in the first place. Both provisions are open to either interpretation—but, based on considerations of fundamental rights, the GDPR and Directive should be interpreted to apply eCommerce Rules to the RTBF.

standard for other forms of liability); Case C-324/09, *L’Oréal SA v. eBay Int’l AG*, 2011 E.C.R. I-6011, ¶ 119.

327. The CJEU’s *L’Oréal* ruling, which confirmed that an injunction could issue against an OSP “regardless of any liability of its own,” reinforces this point. *L’Oréal*, 2011 E.C.R. I-6011, ¶ 127 (applying Directive 2004/48/EC). While the CJEU applied a different Directive in this portion of the ruling, it also applied the intermediary liability provisions of the eCommerce Directive to the same, non-liability-based injunction. *Id.* ¶ 139 (requiring that injunctions comply with the eCommerce Directive prohibition on general monitoring obligations); see also Husovec, *supra* note 49, at 116–18; *Analysis of the Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights in the Member States*, at 16–17, SEC (2010) 1589 final (Dec. 22, 2010), <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010SC1589&from=EN> [<https://perma.cc/Y66Z-7JQL>] (explaining that injunctive relief “granted against the intermediary irrespective whether there has been a determination of liability of the intermediary” is not barred by eCommerce Directive). Further research on the uses of the term “liability” in the intermediary liability context would be instructive.

a) Language in the eCommerce Directive

The eCommerce Directive contains a passage, in Article 1(5)(b), that is widely interpreted as carving out data protection issues from its scope. It says that the eCommerce Directive “shall not apply to . . . questions relating to information society services covered by” data protection law, including the GDPR.³²⁸ Following one interpretation, this would mean that eCommerce Rules do not apply to notice-and-takedown requests that are based on data protection claims—including RTBF requests. In the author’s experience, this reading of Article 5(1)(b) is conventional wisdom among many European practitioners.³²⁹

However, in a 2016 ruling, a Northern Irish appeals court rejected this interpretation. In a case against Facebook, it concluded that intermediary liability is *not* one of the “questions . . . covered by” the 1995 Directive.³³⁰ The court held that the eCommerce Rules apply to notice-and-takedown claims based on data protection, as those rules “do not interfere with any of the principles in relation to the processing of personal data”³³¹ This interpretation is compelling: it makes sense of the language, harmonizes the two sources of law, and preserves balance among affected fundamental rights.

328. eCommerce Directive, *supra* note 12, art. 1(5)(b); *see also* GDPR, *supra* note 6, art. 94(2) (“References to the repealed Directive shall be construed as references to this Regulation.”). An eCommerce Directive Recital suggests that the intermediary liability rules do apply, and must merely be interpreted consistently with data protection requirements: “[T]he implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards . . . the liability of intermediaries” eCommerce Directive, *supra* note 12, recital 14. But it also includes language that could indicate the opposite—that data protection laws simply displace eCommerce rules.

The protection of individuals with regard to the processing of personal data is solely governed by [laws including the 1995 Directive], which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive

Id.

329. *See* Hurst, *supra* note 307 (noting that eCommerce rules “do not on a strict reading of the E-Commerce Directive appear to apply to data protection claims”).

330. *CG v. Facebook Ireland Ltd* [2016] NICA 54, ¶ 93 (Nor. Ir.).

331. *Id.* ¶ 95. Arguably the outcome of this analysis should be different under the GDPR, on the theory that notice-and-takedown procedures are a “question[] . . . covered by” that law—even though they are not covered in the 1995 Directive. *See* eCommerce Directive, *supra* note 12, art. 1(5)(b). This analysis is complicated by language in the GDPR itself, discussed in Subsection IV.B.2.b, that seemingly invokes the eCommerce Directive for RTBF removals.

b) Language in the GDPR

The GDPR invokes the eCommerce Rules directly in Article 2(4), saying that “[t]his Regulation shall be without prejudice to the application of [the eCommerce Directive], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.”³³² At first glance, this seems to expressly apply eCommerce Rules to the RTBF. But the meaning of the passage depends whether the eCommerce “liability rules of intermediary service providers” cover data protection notice-and-takedown in the first place. In other words, it depends on one’s interpretation of eCommerce Directive Article 5(1)(b), discussed above. If the eCommerce Rules do not, by their own terms, apply, then the GDPR could be “without prejudice” to eCommerce Rules simply because each law covers a different set of questions.

That said, if the GDPR drafters were trying to say “these are two unrelated laws,” the above-quoted passage in Article 2(4) would be an odd way to say it. The more natural interpretation is the simpler one: that the GDPR invokes eCommerce Rules for RTBF notice-and-takedown. This would implicitly refute the idea that ordinary intermediary liability law under the eCommerce Directive does not reach RTBF notice-and-takedown. Under this interpretation, the GDPR Rules would remain important and effective for erasure requests that target stored, back-end data. But public, online expression would get the more robust protections of the eCommerce Rules.

3. *Reconciling the eCommerce Directive and Data Protection Law*

One major ruling to date has made a serious effort to reconcile OSPs’ obligations under European intermediary liability and data protection laws. In a case raising data protection claims about a video hosted by Google, Italy’s highest court held that eCommerce Rules applied.³³³ As a result, Google was not legally responsible for the video—which depicted bullying—prior to the time when Google was notified about it and took it down. The Italian court said that Article 5(1)(b) of the eCommerce Directive “does not have the purpose to render the eCommerce provisions inapplicable to any case concerning the protection of personal data.”³³⁴

According to the court, the eCommerce and data protection frameworks can be reconciled by holding that in general the user who posts content—and not the OSP that hosts it—is its controller. The OSP becomes a controller,

332. GDPR, *supra* note 6, art. 2(4); *see also id.* recital 21 (“This Regulation is without prejudice to the application of [the eCommerce Directive] in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.”).

333. Corte di Cassazione, Cass. sez. tre Penale, 3 febbraio 2014, n. 5107/14 (It.).

334. *Id.* ¶ 7.4.

however, once it is notified about user content that violates data protection law:

[A]s long as the service provider is not aware of the unlawful data, the service provider cannot be considered to be the data controller since the provider does not have any decision-making power over the data; on the other hand, if the provider is aware of the unlawful data, and does not do something to immediately remove it or make it inaccessible, the provider then fully takes on the status of data controller, and is therefore subject to the duties and criminal sanctions of [data protection law].³³⁵

This theory, that only OSPs with knowledge are controllers, has some benefits analogous to those of intermediary liability safe harbor laws. Importantly, it relieves OSPs of controller obligations in the time before receiving removal requests. As discussed in Section II.C, classifying OSPs as controllers of every bit of automatically-processed user expression would subject them to illogical or impossible obligations. The Italian court's bright-line rule creates a relatively high degree of legal certainty for OSPs trying to understand their obligations under data protection law. In that sense it is better than *Google Spain's* hazier standard: that a search engine is always a controller, but its obligations are limited to "ensur[ing], within the framework of its responsibilities, powers and capabilities" that it complies with data protection law.³³⁶

Whatever the merits of this framing, however, it does not solve the procedural notice-and-takedown problems created by the GDPR. If an OSP becomes a controller in the moment of receiving a removal request, it still must decide what notice-and-takedown rules to follow: eCommerce Rules or GDPR Rules. The choice has real consequences for the rights of Internet users.

There is another, superficially plausible, variant on the Italian court's approach that raises still more problems. It could be argued that controllers

335. *Id.* ¶ 7.2. In another dispute raising the issue in 2015, a UK court stated a "provisional preference" for the conclusion that "the two Directives must be read in harmony and both, where possible, must be given full effect to." *See Mosley v. Google Inc.*, [2015] EWHC (QB) 59 [45]–[46] (describing but not resolving the question of whether eCommerce Rules apply to data protection claims). This case, which the author worked on as counsel to Google, concerned a plaintiff's request for Google to proactively filter images from web search results, based on privacy and data protection rights. *See id.*; *see also* Sophie Stalla-Bourdillon, *Data Protection & Intermediary Liability: How Do the French Do It?*, PEEP BEEP! (Apr. 1 2017), <https://peepbeep.wordpress.com/2017/04/01/data-protection-intermediary-liability-how-do-the-french-do-it/> [<http://perma.cc/UUQ8-MLKM>] (describing a French case that recognized applicability of eCommerce Rules in data protection claim against blogging platform for content posted by users).

336. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317, ¶ 3.

never fall within the eCommerce safe harbors, because in determining the “purposes and means” of processing user-generated content, they take a role too active to qualify for immunity under the Directive. Conflating the data protection and eCommerce classifications in this manner would in theory align the two frameworks as follows:

Data processors under 1995 Directive or GDPR	=	Immunized “passive” OSPs under eCommerce Directive
---	---	---

Data controllers under 1995 Directive or GDPR	=	Non-immunized “active” OSPs under eCommerce Directive
--	---	--

This equation has troubling consequences for both areas of law, though. For one thing, it would strip OSPs of intermediary liability protection for claims entirely unrelated to data protection. Following this theory, *Google Spain’s* holding that Google is a controller would mean that the search engine is too “active” to qualify for eCommerce Directive defenses for copyright claims, defamation claims, and much more. This would not only be bad policy, it would be inconsistent with cases and laws establishing that Google’s search engine *does* qualify for eCommerce Directive defenses.³³⁷

Similarly, data protection rules need to cover a vast array of issues unrelated to notice-and-takedown, from employer record-keeping to online targeted advertising. Court rulings in eCommerce cases about unrelated issues, like trademark claims or hate speech, should not have the unintended consequence of distorting data protection regulation. The eCommerce active/passive distinction and data protection’s controller/processor distinction are themselves moving targets within two separate, complex, and rapidly changing legal fields. The evolution of the two bodies of law should not be distorted by hitching their key classifications together.

Finally, conflating the two classification systems would not address the problems with RTBF notice-and-takedown. It would put the very OSPs that must honor RTBF requests—controllers—outside of the eCommerce Directive’s intermediary liability framework, and effectively strip Internet users of key legal protections against over-reaching RTBF removal demands.

337. See *supra* note 52. To be clear, inconsistent case law in EU countries is not necessarily a “conflict” in the U.S. legal sense. National law implementing the eCommerce Directive can vary, and civil law courts can depart from precedent more than common law courts.

V. SOLUTIONS

This Article has detailed the unnecessary risks of the GDPR's notice-and-takedown provisions and has suggested legal arguments to mitigate them. This final Section briefly distills those arguments into specific proposed solutions.

The most immediate avenue for improving the GDPR is through actions of the new Board or Member State legislators. Both will have critical opportunities to shape real-world OSP behavior through laws and guidelines they publish. Member States, which are mandated to pass laws balancing free expression with the new GDPR rights, can enact important limitations within their own jurisdictions. The Board can issue and refine EU-wide guidelines for DPAs, OSPs, and data subjects who send RTBF requests. In consultation with EU intermediary liability and free expression rights experts, both could arrive at well-crafted, balanced approaches.

A second means of improving GDPR notice-and-takedown is through disputes and litigation before DPAs or courts. This approach would likely lead, at best, to piecemeal resolution of the problems described here. But for problems that are not addressed by Board or Member State action, dispute resolution through DPAs and courts may be the best remaining option.

A. RULES FROM THE ECOMMERCE DIRECTIVE SHOULD GOVERN NOTICE-AND-TAKEDOWN UNDER THE GDPR

This Article argues that the notice-and-takedown regime described in the GDPR tilts the playing field against users seeking and imparting information online. For example, the GDPR "restriction" provisions encourage OSPs to take content offline even for invalid RTBF requests. By contrast, the eCommerce Directive requires removal only for adequately substantiated legal claims. For RTBF requests targeting public, online information, the eCommerce Directive is a better source of procedural law than the GDPR.³³⁸ Adopting rules based on the eCommerce Directive would be the simplest solution to the "restriction" issue and an array of other problems identified in Section III.C of this Article. The Board's notice-and-takedown guidelines could easily track the protections of the eCommerce Directive, and even offer improvements over Member States' current implementations.³³⁹ Article 2(4) of the GDPR provides a simple legal basis for doing so.³⁴⁰ This interpretation would leave the GDPR's provisions intact and effective for erasure of back-end, privately held data such as user accounts or ad-targeting profiles.

338. See *supra* Sections III.B, IV.A.

339. See *Single Market Online Services*, *supra* note 37, at 44–46 (identifying issues and areas for improvement in eCommerce notice-and-takedown procedures).

340. See *supra* Section IV.B.2.b).

B. IF GDPR RULES APPLY TO NOTICE-AND-TAKEDOWN, THEY SHOULD BE INTERPRETED TO MAXIMIZE PROCEDURAL FAIRNESS

If lawmakers do not invoke eCommerce Rules for erasure of public online content, the next best hope is to interpret GDPR Rules in a way that restores a measure of balance between the different fundamental rights affected by notice-and-takedown of online information. Interpretations along these lines are discussed in Section III of this Article. For example, lawmakers could determine that requests to temporarily “restrict” access to online data while an OSP reviews a data subject’s erasure request do not apply to online expression, or apply only in narrowly defined cases.³⁴¹ The challenge with this approach arises from reliance on potentially strained interpretations of GDPR text. For example, it is hard to come up with alternate interpretations of provisions that seem to require OSPs to disclose personal data about online speakers.³⁴² Without the clean sweep displacement of GDPR rules by eCommerce rules, protection for online speakers would depend on piecemeal interpretation of each problematic GDPR provision.

C. HOSTS SHOULD NOT BE SUBJECT TO RTBF OBLIGATIONS

Excluding hosting services from obligations to erase users’ online expression would mitigate one of the greatest potential threats to information rights under the GDPR. As discussed in Section III.B, governing law on this topic is extremely open to interpretation. Hosts, including social media services, could be controllers or not. The reasoning of *Google Spain* could apply to them in part or not at all. Regardless of how these questions are resolved, hosts will continue to have removal obligations for other claims, including defamation and privacy torts.

If hosts did have to remove content based on RTBF claims, they clearly would need to follow different rules than the ones applied to search engines. As *Google Spain* made clear, data can lawfully remain on a website even when the RTBF applies to the same data in search results. And since hosts ranging from Twitter to DropBox may be the only online source—or the only source, full stop—for expression or information, the consequences of erasure are more significant. New guidance would be required both for hosts’ substantive standards in weighing the public interest against RTBF requests, and their technical implementation of erasure.

Uncertainty about hosts’ obligations and the RTBF creates particularly strong risks of over-removal, because hosts will be motivated to avoid disputes that could lead DPAs to determine that they are controllers. A clear message

341. See *supra* Section III.C.I.I.A.2.

342. See *supra* Section III.C.4.b.

that hosts will not be held to RTBF obligations, even if temporarily, could minimize this threat to Internet users' expression and information rights.

D. DPAs SHOULD NOT ASSESS FINANCIAL PENALTIES AGAINST OSPs THAT REJECT RTBF REQUESTS IN GOOD FAITH

Fear of high fines gives OSPs reason to readily remove user-generated content, even if the request for removal is over-reaching and unsupported by European law. The combination of perceived or real financial pressure with unclear legal rules is dangerous for information rights, as discussed in Section III.A. Lawmakers could protect ordinary Internet users and bring OSPs' incentives into better balance by assuring OSPs, clearly and in writing, that they do not risk fines when they reject questionable RTBF requests or preserve procedural notice-and-takedown protections for their users.

Such an assurance would not turn indifferent OSPs into defenders of users' rights, since standing up for them would still impose costs in time, lawyers' fees, or exposure to regulatory attention. But for those with limited resources and a desire to protect users, it could make a very important difference.

E. EU MEMBER STATE LAW AND REGULATORY GUIDANCE SHOULD ROBUSTLY PROTECT FREEDOM OF EXPRESSION IN RTBF CASES

The GDPR expressly charges Member States with protecting free expression, and mandates that DPAs broadly protect fundamental rights and freedoms of all sorts.³⁴³ On this basis, either or both could establish thoughtful, substantive standards to guide OSPs considering which RTBF requests to honor. Such standards will be particularly important for hosts, if they are deemed controllers, since existing guidance for search engines is inappropriate for them and would lead to over-removal of lawful content.³⁴⁴ Free expression rights can also be protected through procedural rules discussed throughout this Article.

F. JURISDICTIONAL RULES SHOULD RESPECT NATIONAL LEGAL DIFFERENCES

The GDPR respects the diversity of Member State law on free expression and information, calling on each country to enact its own laws balancing those rights with data protection.³⁴⁵ But it leaves open questions about the territorial scope of enforcement and whether one country can effectively impose its laws on others—both within and outside the EU. The CJEU will soon speak to this

343. GDPR, *supra* note 6, arts. 51(1), 85; *see also* Keller, *supra* note 266.

344. *See supra* Sections III.C, III.B.

345. *See supra* Section III.E; GDPR, *supra* note 6, art. 85.

issue, and policymakers may not want to address it before the court does. To the extent that the case outcome leaves room for further interpretation, though, policymakers should balance the interests of all affected parties and states to ensure that no one fundamental right always prevails over the others when national laws diverge. As discussed in Section III.E, current legal pressures and OSP responses risk prioritizing privacy over information rights in this situation, leading to EU-wide and perhaps global enforcement of the most information-restrictive rules. Technical tools for limited geographic enforcement of national laws, including geographic service targeting or blocking by OSPs, should be considered.

VI. CONCLUSION

Privacy and information rights are, in principle, equally important and proportionally protected under EU law. Balance between the two rights is necessary to support both individual and collective rights to liberty and democratic participation.

The GDPR unintentionally but seriously disrupts this balance, tilting the playing field in favor of privacy rights and the individuals who assert them. It does so through seemingly innocuous procedural rules for data controllers—rules which, when applied to OSPs' notice-and-takedown systems for public online speech, systematically favor erasure.

The result is a powerful new tool for abusive claimants to hide information from the public. Bloggers documenting misuse of power can be silenced, and small businesses can lose access to customers, all through secret accusations sent to private technology companies. For RTBF claims that raise genuinely hard-to-resolve questions about data protection and the public interest, the GDPR's rules systematically push toward removing or de-listing information. As few of these decisions will ever reach public adjudication, the de facto rules governing a vast swath of online expression will be defined by risk-averse OSPs interpreting ambiguous provisions of the GDPR.

The good news is that much of this harm can be avoided without sacrificing the data protection and privacy rights safeguarded by the GDPR. Existing law under the eCommerce Directive and the EU's fundamental rights framework provides the tools. Using these tools, policymakers can guide OSPs in striking a better balance and protecting both privacy and information rights online.