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.

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 27 NUMBER 1 SPRING 2012

TABLE OF CONTENTS

ARTICLES

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., 19th ed. 2010). Please cite this issue of the *Berkeley Technology Law Journal* as 27 BERKELEY TECH. L.J. ___ (2012).

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*, and the Bolt, a collection of short comments and updates about new developments in law and technology written by members of BTLJ.

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 Express*O* 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 Express*O* 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., 19th ed. 2010).

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.

MESSAGE TO SUBSCRIBERS

Welcome to the first issue of Volume 27 of the *Berkeley Technology Law Journal*. With this volume, the Journal continues distribution of the regular Spring, Fall, and Symposium issues but is ceasing subscriber distribution of the Annual Review of Law and Technology. The Spring issue will now begin each volume. The Annual Review, which publishes student-written work surveying recent developments in law and technology, will follow in online format only. Subscribers may always download the current and past Annual Reviews at http://www.btlj.org and find them on HeinOnline, LexisNexis, and Westlaw. The Journal will then distribute in print the Fall issue and finish the volume with the Symposium issue, which contains pieces contributed by participants at the annual law and technology Symposium organized jointly by the Berkeley Center for Law and Technology and the Journal and held at the University of California, Berkeley School of Law every spring. With these changes, we look forward to continuing to provide you with timely publication of cutting-edge and influential scholarship in law and technology.

2011–12 Executive Committee
Berkeley Technology Law Journal

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

FENWICK & WEST LLP

ORRICK, HERRINGTON & SUTCLIFFE LLP

Benefactors

COVINGTON & BURLING LLP

FISH & RICHARDSON P.C.

KASOWITZ BENSON TORRES & FRIEDMAN LLP

KIRKLAND & ELLIS LLP

LATHAM & WATKINS LLP

MCDERMOTT WILL & EMERY

MORRISON & FOERSTER LLP

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

WEIL, GOTSHAL & MANGES LLP

WHITE & CASE LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

WILSON SONSINI GOODRICH & ROSATI

WINSTON & STRAWN LLP

Members

ALSTON + BIRD LLP

BAKER BOTTS LLP

BINGHAM MCCUTCHEN LLP

DEWEY & LEBOEUF LLP

DURIE TANGRI LLP

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP

GUNDERSON DETTMER STOUGH VILLENEUVE FRANKLIN & HACHIGIAN, LLP

HAYNES AND BOONE, LLP

HICKMAN PALERMO TRUONG BECKER, LLP

KEKER & VAN NEST LLP

KILPATRICK TOWNSEND & STOCKTON LLP

KNOBBE MARTENS OLSON & BEAR LLP

MORGAN, LEWIS & BOCKIUS LLP

MUNGER, TOLLES & OLSON LLP

ROPES & GRAY LLP

SCHWEGMAN LUNDBERG WOESSNER

SIDLEY AUSTIN LLP

VAN PELT, YI & JAMES LLP

WEAVER AUSTIN VILLENEUVE & SAMPSON, LLP

Patrons

BAKER & MCKENZIE

BOARD OF EDITORS 2011–2012

Executive Committee

Editor-in-Chief
TARAS M. CZEBINIAK

Managing Editor
MICHELLE MA

Senior Articles Editors
AARON MACKEY
MILES PALLEY
ARIELLE SINGH

Senior Executive Editor
WYATT GLYNN

Senior Annual Review Editors
RYAN IWAHASHI
BRITT LOVEJOY

Senior Scholarship Editor
ALEXANDER REICHER

Editorial Board

Submissions Editors
DANIEL KAZHDAN
ZACHARY MARKARIAN

Production Editors
JARAD BROWN
LAUREN SIMS

Bluebook Editors
JILLIAN FEINBERG
CONRAD GOSEN
MIKE SHEEN

Annual Review Editors
ROSS BARBASH
REZA DOKHANCHY

Notes & Comments Editors
COURTNEY BOWMAN
WINNIE HUNG

Symposium Editors
CIARA MITTAN
KILEY WONG

Web Content Editor
MICHAEL SOBOLEV

Information Management Editor
ANDREW FONG

Web & Technology Editor
ANDREA YANKOVSKY

External Relations Editor
ARIANA GREEN

Publishing Editor
NICK WOLOSZCZUK

Member Relations Editor
JEN SPENCER

Articles Editors

LAUREN ESCHER
AMY HAYDEN
KAREN KOPEL
RUBINA KWON
YVONNE LEE
JANE LEVICH
ANGELA MAKABALI
TAYLOR MARGOT
NIKHIL MATANI
HANNAH MINKEVITCH
SONYA PASSI
DAVID ROSEN
JOE SEXTON

MEMBERSHIP

Vol. 27 No. 1

Associate Editors

ARUSYAK ABRAHAMYAN	GRANT GARBER	LALITHA MADDURI
JULIE BYREN	CASEY HULTIN	MARIENNA MURCH
EMILY CHEN	DAMION JURRENS	JEAN PAUL NAGASHIMA
SHRUTI CHOPRA	GARY JUSKOWIAK	JUSTIN ORR
KEYNA CHOW	RYAN KLIMCZAK	SARAH ORRICK
ROSS COHEN	JESSE KOEHLER	DINA ROUMIANTSEVA
ANGEL DIAZ	JULIA KOLIBACHUK	MANE SARGSYAN
CHRISTINA FARMER	CLAUDIA LANGER	LAUREN SMITH
NATALIE FLECHSIG	ALEX LI	JENNIFER TRUONG
BENJAMIN FOX	NICOLE LUEDDEKE	PENNI TAKADE
NICOLE A. FRITZ	GAVIN LIU	ROBERT UNDERWOOD
HILARY FRUITMAN		KENNETH VILLA

Members

SAMIRA ANFI	FUMIYO DOI	CODY LONNING
CRAIG ARMSTRONG	MATTHEW DONOHUE	CHRIS MACIEL
JENNIFER BARNETTE	ELISE EDLIN	RENUKA MEDURY
ERIK BAUMAN	ALAN ENRIQUEZ	KEVIN MEIL
ZACH BARON	MAKOTO FURUYA	EDUARD MELESHINSKY
KEVIN BENDIX	JOSHUA GLUCOFT	MIKI NAITO
CAROLYN BLUMENFELD	FELICITY GRISHAM	JOHN OWEN
TRISTAN BROWN	BRITT HARWOOD	GLORIA POON
NORMA CERROS	KEIGO HIDAKA	FELIX PRUEMMER
CHRISTINA CHAREMI	NAOMI HUNG	JINGWEN REN
DENA CHEN	GWYNNE HUNTER	SANDRA SANZ
JOSIE CHEN	JESSICA KENNY	SEAN SHIH
CHRIS CIVIL	PUNEET KOHLI	MICHAEL SU
NOAM COHEN	MILA KONOVALCHUK	PRISCILLA TAYLOR
PAUL COX	ROBIN KUNTZ	EDWARD TOROUS
ERIC CUELLAR	NICHOLAS LAMPROS	YUE WANG
KARAN DHADIALLA	NICK LEEFER	ETHAN WEINER
LUIZA DIAS	SENTA LEYKE	HAILEY YOU

BTLJ ADVISORY BOARD

BERKELEY CENTER FOR LAW & TECHNOLOGY 2011–2012

Executive Director
ROBERT BARR

Faculty Directors
PETER MENELL
ROBERT MERGES
DEIRDRE MULLIGAN
PAMELA SAMUELSON
PAUL SCHWARTZ
SUZANNE SCOTCHMER
MOLLY VAN HOUWELING

Associate Director
LOUISE LEE

Assistant Director
JULIA TIER

Affiliated Faculty and Scholars

AARON EDLIN
JOSEPH FARRELL
RICHARD GILBERT
BRONWYN HALL
THOMAS JORDE
MICHAEL KATZ
DAVID MOWERY
DAVID NIMMER
DANIEL RUBINFELD
ANNALEE SAXENIAN
JASON SCHULTZ
HOWARD SHELANSKI
CARL SHAPIRO
MARJORIE SHULTZ
LON SOBEL
TALHA SYED
DAVID TEECE
JENNIFER M. URBAN
HAL R. VARIAN
DAVID WINICKOFF

ANTICOMPETITIVE INNOVATION AND THE QUALITY OF INVENTION

Alan Devlin[†] *& Michael Jacobs*[††]

ABSTRACT

When, if ever, should antitrust condemn an act of invention? This Article addresses the challenging question of how best to judge predatory-invention claims, and under what standard courts should go about the formidable task of weighing the quality of a challenged improvement. It rejects as variously unworkable, incongruous, or incomplete the conflicting legal standards espoused by the D.C., Second, Ninth, and Federal Circuits.

After considering several pertinent issues, the Article advocates the following test: if an impugned act of invention does not foreclose, but merely disadvantages, rival products, it should be per se lawful. If the challenged innovation effectively excludes entry into the relevant market, an antitrust violation should follow if the plaintiff demonstrates, and the defendant fails to rebut, the absence of a genuine technological improvement. The Article defines "genuine" as reflecting a calculable premium that consumers would pay for the improved-upon alternative(s), even if the extent of that price differential falls short of the level required to place the new product in a distinct antitrust market.

In determining the quality of an invention, courts should not draw an inference of technological merit from the fact that the U.S. Patent & Trademark Office has issued a patent, nor should evidence of predatory intent play a role in the analysis. The Article also recommends jettisoning from antitrust analysis the concept of "coercion." The Article concludes by applying its test to the quintessential example of predatory innovation: product hopping in the pharmaceutical industry.

---

† Associate, Latham & Watkins LLP. B.B.L.S. (Int'l), University College Dublin (2004); L.L.M., University of Chicago Law School (2005); J.S.D., University of Chicago Law School (2006); J.D., Stanford Law School (2007).

†† Distinguished Research Professor of Law, DePaul University College of Law. B.A., Dartmouth College (1968); J.D., Yale Law School (1971).

The views expressed in this Article are solely those of the authors.

TABLE OF CONTENTS

I. INTRODUCTION

That the law should promote innovation is an unquestioned precept of modern public policy.[1] Economists continue to debate which form of industrial organization—competition or monopoly—encourages more innovation.[2] However, the vast majority have long agreed that the economic benefits flowing from invention dwarf those from all other sources of economic advancement combined.[3] Yet, plaintiffs routinely challenge the "predatory" inventions of dominant firms on the ground that these inventions wrongfully exclude small rivals in violation of the antitrust laws.[4] The questions of whether and when the law should condemn such instances of technological improvement are among the most divisive in the field of competition policy today.[5]

Lawsuits alleging predatory innovation implicate complex policy questions, such as the nature of invention; the difficulties of comparing the long-term benefits of bona fide technological improvements with short-term harms that might arise when a dominant firm excludes a smaller rival; and issues of institutional competence. A larger question asks whether courts should entertain such claims at all. If they do hear such cases, should the judiciary evaluate claims of improvement by looking to consumer purchasing decisions, by deferring to the decision of the U.S. Patent and Trademark

1. *See, e.g.*, U.S. DEP'T OF JUSTICE (DOJ), COMPETITION AND MONOPOLY: SINGLE-FIRM CONDUCT UNDER SECTION 2 OF THE SHERMAN ACT 1 (2008), *available at* http://www.usdoj.gov/atr/public/reports/236681.pdf (observing that innovation is "the most important source of economic growth").

2. This debate is best encapsulated by the long-running dispute between Joseph Schumpeter and Kenneth Arrow as to whether monopoly or competition is the best driver of technological advancement. *Compare* JOSEPH A. SCHUMPETER, CAPITALISM, SOCIALISM, AND DEMOCRACY (3d ed. 1950), *with* Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* NAT'L BUREAU OF ECON. RESEARCH, THE RATE AND DIRECTION OF INVENTIVE ACTIVITY: ECONOMIC AND SOCIAL FACTORS 609 (1962).

3. *See, e.g.*, ARTI RAI, STUART GRAHAM & MARK DOMS, U.S. DEP'T OF COMMERCE, PATENT REFORM: UNLEASHING INNOVATION, PROMOTING ECONOMIC GROWTH & PRODUCING HIGH-PAYING JOBS 1 (2010), *available at* http://www.commerce.gov/sites/default/files/documents/migrated/Patent_Reform-paper.pdf (linking innovation to three-quarters of the U.S. economy's post-World War II growth).

4. *See* cases discussed *infra* Section II.B.

5. The single most divisive recent case implicating this tension involved the United States and European Union proceedings against Microsoft. *See generally* WILLIAM H. PAGE & JOHN E. LOPATKA, THE MICROSOFT CASE: ANTITRUST, HIGH TECHNOLOGY, AND CONSUMER WELFARE (2007). More generally, see Claudette Espanol, *The Federal Circuit: Jurisdictional Expansion into Antitrust Issues Relating to Patent Enforcement*, 2 SETON HALL CIRCUIT REV. 307, 307–08 (2005); Michael J. Meurer, *Vertical Restraints and Intellectual Property Law: Beyond Antitrust*, 87 MINN. L. REV. 1871, 1871–76 (2003).

Office ("PTO") to grant a patent, by appealing to expert testimony from engineers and scientists in the field, or by some combination of these?

The proper substantive test for evaluating such inventions is hardly self-evident. Should a modicum of improvement shield the defendant from antitrust liability, or should legality turn on the outcome of a cost-benefit analysis that weighs the value of the improvement against the cost of suppressed competition? These questions are made more difficult by long-debated issues concerning the industry structure that best fosters innovation.[6] Perhaps most importantly, the courts' systemic capacity to err in quantifying the social value of an invention, as well as its short- and long-run competitive effects, necessitates a central role for decision theory.[7] But what form should that theory take? Deeming a material propensity for Type I errors ("false positives") to be unacceptable in light of the perverse incentives generated by condemning socially valuable innovation, one might err strongly on the side of permissibility.[8] Those who are sanguine about courts' ability to distinguish nugatory from genuine acts of invention, however, might seek to reduce the incidence of Type II errors ("false negatives") by taking claims of predatory innovation more seriously.[9]

Famous examples of allegedly anticompetitive innovation abound. In the 1970s, Kodak launched its successful Kodacolor II system, which used a new camera format and film that disadvantaged Kodak's competitors in the film and photofinishing markets. Kodak's actions led these competitors to argue that antitrust law should impose a duty on dominant firms to disclose technological changes in advance if they could harm rivals.[10] In the same decade, competitors accused IBM of designing its products to render them

6. *See supra* note 2; *see also* Jonathan B. Baker, *Beyond Schumpeter Versus Arrow: How Antitrust Fosters Innovation*, 74 ANTITRUST L.J. 575 (2007); Michael A. Carrier, *Two Puzzles Resolved: Of the Schumpeter-Arrow Stalemate and Pharmaceutical Innovation Markets*, 93 IOWA L. REV. 393, 396 (2008) (discussing the status of the debate). *See generally* Harry S. Gerla, *Restoring Rivalry as a Central Concept in Antitrust Law*, 75 NEB. L. REV. 209 (1996); Richard Gilbert, *Looking for Mr. Schumpeter: Where Are We in the Competition-Innovation Debate?*, 6 INNOVATION POL'Y & ECON. 159 (2006).

7. *See generally* Frank H. Easterbrook, *The Limits of Antitrust*, 63 TEX. L. REV. 1 (1984); Geoffrey A. Manne, *Innovation and the Limits of Antitrust*, 6 J. COMPETITION L. & ECON. 153 (2010).

8. *See, e.g.*, Thomas B. Leary, *The Essential Stability of Merger Policy in the United States*, 70 ANTITRUST L.J. 105, 134–35 (2002); D. Daniel Sokol, *Antitrust, Institutions, and Merger Control*, 17 GEO. MASON L. REV. 1055, 1062 (2010).

9. A Type I error, or false positive, occurs in this context when a court mistakenly condemns as anticompetitive an invention that promotes long-run consumer welfare discounted to present value. A Type II error, or false negative, takes place when a court finds that an anticompetitive innovation does not violate the antitrust laws.

10. *See* Berkey Photo, Inc. v. Eastman Kodak Co., 603 F.2d 263, 279 (2d Cir. 1979).

incompatible with the competitors' goods.[11] In the late 1990s, Microsoft's bundling of its operating system and Internet-browsing software (a technological tie-in) resulted in serious antitrust liability.[12] Most recently, Google's quest to scan all of the world's books and to make them searchable online—an innovation of epic proportion—ran into antitrust trouble when the company sought to settle a class-action lawsuit alleging massive copyright infringement.[13] The U.S. District Court for the Southern District of New York refused to approve the settlement, in part because it would grant Google, but not its competitors, rights over so-called "orphan works" (in-copyright works for which the rights holders are unidentifiable).[14]

This Article argues that the law should decline to entertain an antitrust challenge where the impugned invention, modest though it may be, does not prevent the marketing of rival products. But where the challenged innovation forecloses market entry, thus eliminating rather than simply reducing consumer choice, this Article advocates a standard that would render the impugned behavior illegal if a plaintiff proves, and the defendant fails to rebut, the absence of a genuine technological improvement. A "genuine" improvement in this context is a feature that consumers would pay a premium to acquire, though the necessary premium is less than the five to ten percent over the existing price that often accompanies market-definition analysis.[15] Under this proposed standard, an exclusionary "invention" that transforms a product into a pure substitute in the eyes of consumers would violate the antitrust laws.[16]

---

11. *See* Memorex Corp. v. IBM, 636 F.2d 1188 (9th Cir. 1980) (per curiam); Cal. Computer Prods. v. IBM, 613 F.2d 727, 731 (9th Cir. 1979); *In re* IBM Peripheral EDP Devices Antitrust Litig., 481 F. Supp. 965 (N.D. Cal. 1979), *aff'd*, 698 F.2d 1377, 1382 (9th Cir. 1983).

12. *See* United States v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001).

13. Authors Guild v. Google Inc., 770 F. Supp. 2d 666, 669 (S.D.N.Y. 2011). A number of prominent scholars argued that the Google Books Search settlement would have created antitrust issues, though other leading academics disagreed. *Compare, e.g.*, Randal C. Picker, *The Google Book Search Settlement: A New Orphan-Works Monopoly?*, 5 J. COMPETITION L. & ECON. 383 (2009), *and* Pamela Samuelson, *Google Book Search and the Future of Books in Cyberspace*, 94 MINN. L. REV. 1308 (2010), *with* Einer Elhauge, *Why the Google Books Settlement Is Procompetitive*, 2 J. LEGAL ANALYSIS 1 (2010), *and* Jerry A. Hausman & J. Gregory Sidak, *Google and the Proper Antitrust Scrutiny of Orphan Books*, 5 J. COMPETITION L. & ECON. 411 (2009).

14. *Authors Guild*, 770 F. Supp. 2d at 682–83.

15. Given patent law's minimalist reading of the utility requirement, we would not view the fact that the PTO has issued a patent to be sufficient proof of a genuine improvement.

16. Thus, if consumers mistakenly pay a premium for a new product over a withdrawn product based on what they erroneously perceive to be a qualitatively material improvement, no antitrust violation would result under this Article's proposed test. As explained below, the disproportionate costs of erroneously condemning real acts of invention (Type I errors)

Thus, the elimination, rather than the reduction, of consumer choice should be a prerequisite of an antitrust violation. Imagine that consumers, through their purchasing decisions, were to signal a greater preference for a dominant firm's purportedly "improved" product than for a rival plaintiff's product. Under this Article's proposed test, such a product introduction would necessarily be lawful, even if market research demonstrated that the "premium" for the improved good resulted entirely from marketing and advertising, rather than from a technologically cognizable improvement.

One might be tempted to expand the scope of potential illegality by adopting the principle that consumer choice is not meaningful when it is fettered, or otherwise subject to some "improper" influence. One would then entertain antitrust claims against an "improved" good for which consumers display a predilection when their demand is in some respect irrational, or skewed by market conditions or by the defendant's own conduct. This Article rejects such an approach because it would eliminate a meaningful role for consumers in judicial assessments of the legitimacy of an innovation. Myriad influences invariably hinder consumers' ability to act as perfectly neutral and accurate arbiters of technological quality, even in competitive markets. In the consumer-focused field of antitrust, however, the individual purchasers' market-revealed preferences are entitled to deference, and courts ought not to second-guess them ex post. It is only where an alleged act of predatory innovation denies consumers a choice between rival products that rule-of-reason analysis is appropriate.

A necessary result of this standard is that, over time, some inventions that produce long-run social costs will escape antitrust condemnation.[17] This is the necessary price for ensuring that exclusivity continues to operate as an appropriate mechanism for rewarding invention. A more open-ended antitrust standard, which might employ an all-encompassing cost-benefit calculus to determine legality, would do great harm to legal certainty and thus create an unacceptable risk of corrupting innovation incentives.

To explore this thesis, the Article applies our analysis to what many might consider to be the quintessential example of predatory innovation: "product hopping." Product hopping occurs when a pioneer pharmaceutical firm switches consumers from one form or dosage of its product—typically, a product for which the patent will soon expire—to another form or dosage

justify an antitrust standard that deliberately accepts a relatively greater incidence of Type II errors. *See infra* Section IV.C.

17. *See, e.g.*, Lawrence M. Frankel, *The Flawed Institutional Design of U.S. Merger Review: Stacking the Deck Against Enforcement*, 2008 UTAH L. REV. 159, 159 (observing that under-enforcement results in a "greater number of false negatives than false positives").

of that product, in order to maintain the product's profitability. This behavior usually occurs at the expense of competition from a generic prepared to compete with the original formulation.[18] Some consider this practice to be both bereft of plausible benefit and unfairly manipulative of the statutory framework governing the marketing of pharmaceuticals.[19] Nevertheless, consistent with our proposed rule, this Article argues that this practice should be lawful when it leaves generic-drug producers free to enter the market. Moreover, because the phenomenon of product hopping is the natural result of the regulatory infrastructure applicable to the pharmaceutical industry, in most instances, it does not lend itself to an effective judicial solution.[20]

In sum, the problem of anticompetitive innovation is a confoundingly difficult one. The U.S. Supreme Court has never ruled on a case involving predatory innovation. Since the late 1960s, however, various circuit courts of appeals have decided a significant number of such cases.[21] None of those decisions offer a coherent approach to the perceived problem of predatory innovation, and some are downright confusing. Each decision suffers from the same dilemma: assuming that the new product differs in some respect from the old one, how is a court to determine whether that difference offers consumers a benefit sufficient to justify the short-term loss of competition? Is any benefit enough? Or must it exceed some quantitative or qualitative baseline? And who is to judge the fact and nature of the alleged benefit—the court? consumers? technical experts? the PTO?

This Article seeks to provide some answers to those questions. Part II discusses the phenomenon of predatory innovation and critiques the leading case law that has addressed that issue. Part III identifies three factors that courts have used to shed light on the question of whether a product design is predatory, and it explains why the law should revisit those factors. Part IV articulates our preferred legal rule for analyzing alleged instances of exclusionary invention. Part V deals with product hopping as an industry-specific example of predatory innovation—one that presents the same analytical problems as the general-run cases, and that, like them, has no easy solution. A brief conclusion follows.

18. *See, e.g.*, Michael A. Carrier, *Provigil: A Case Study of Anticompetitive Behavior*, 3 HASTINGS SCI. & TECH. L.J. 441, 446–48 (2011).

19. *See infra* note 180.

20. *See infra* Part V.

21. *See supra* note 11.

II. JUDICIAL ANALYSIS OF PREDATORY INNOVATION

A. THE PARADOX OF HARMFUL INNOVATION

Claims of "anticompetitive innovation"[22] sound oxymoronic. As innovation is of exceptional economic importance—a 2010 report by the U.S. Department of Commerce tied three-quarters of U.S. post-World War II economic growth to innovation[23]—one might plausibly think that the judiciary should never condemn it. Yet, the law bears the potential to stymie invention and the growth that it produces.[24] This follows from the fact that one company's successful invention may seriously disadvantage its rivals or even render them insolvent.[25] Rivals thus aggrieved will predictably seek recompense through the legal system, if permitted to do so.[26] An antitrust policy that is both uncritically hostile to monopolization and devoted to ensuring viable competition through equality of opportunity may wrongly condemn inventions that fortify inventors' dominance.[27] Competition policy must be alert to this threat, and courts should summarily reject allegations of monopolization founded on acts of genuine invention.[28]

Claims of antitrust harm arising from consumer-pleasing acts of innovation are necessarily ill founded. But what should the law make of allegations that a dominant defendant strategically engaged in illusory acts of

22. *See, e.g.*, John E. Lopatka, United States v. IBM*: A Monument to Arrogance*, 68 ANTITRUST L.J. 145, 157–58 (2000).

23. RAI, GRAHAM & DOMS, *supra* note 3.

24. *See, e.g.*, Ronald A. Cass, *Copyright, Licensing, and the "First Screen,"* 5 MICH. TELECOMM. & TECH. L. REV. 35, 70 (1999) (noting the danger that "the antitrust laws [have] become captive of well-placed firms in search of an industrial policy that protects declining firms against more successful firms—an outcome likely to frustrate innovation").

25. *See, e.g.*, Herbert Hovenkamp, *Exclusive Joint Ventures and Antitrust Policy*, 1995 COLUM. BUS. L. REV. 1, 24 ("Innovation injures non-innovating rivals of the innovated product even if these rivals were formerly behaving competitively. . . . It may even put some or even all of the makers of the older product out of business.").

26. *See* Joseph F. Brodley, *Antitrust Standing in Private Merger Cases: Reconciling Private Incentives and Public Enforcement Goals*, 94 MICH. L. REV. 1, 49 (1995); *see also* Daniel A. Crane, *Antitrust Antifederalism*, 96 CALIF. L. REV. 1, 39 (2008) (noting that "[a]bout two-thirds of private enforcers of antitrust are aggrieved competitors or other businesses vertically related to the defendant").

27. This follows in part from the fact that distinguishing predatory from efficient conduct is far from straightforward. *See, e.g.*, Frank H. Easterbrook, *On Identifying Exclusionary Conduct*, 61 NOTRE DAME L. REV. 972, 972 (1986) ("Aggressive, competitive conduct by a monopolist is highly beneficial to consumers. Courts should prize and encourage it under the antitrust laws. Aggressive, exclusionary conduct by a monopolist is deleterious to consumers. Courts should condemn it under the antitrust laws. There is only one problem. Competitive and exclusionary conduct look alike.").

28. *See, e.g.*, John E. Lopatka & William H. Page, *Posner's Program for the Antitrust Division: A Twenty-Five Year Perspective*, 48 SMU L. REV. 1713, 1736–37 (1995).

innovation—i.e., those lacking technological merit or any cognizable qualitative improvement over a prior product—in order to exclude rivals? As a threshold matter, one might question the plausibility of any such claim because the competitive harm suffered by an inventor's competitors is directly related to the quality of the relevant invention. After all, one company's revolutionary invention can drive its competitors into bankruptcy and create a monopoly.[29] Conversely, the more prosaic the marketed innovation, the less significant the competitive disadvantage suffered by the innovator's rivals.[30] Such principles might suggest that courts should categorically reject claims of "predatory innovation," for genuine exclusion is plausible only where a new technology renders competitors' products partially or largely defunct.

Are all claims of predatory innovation therefore spurious? At least as a matter of theory, the answer is no.[31] Under certain conditions, trivial acts of invention can exclude rivals on qualitatively improper grounds.[32] When consumers are incapable of effectively distinguishing between various technologies, or when a regulatory mechanism governing entry lends itself to manipulation, strategic product development may frustrate rivals' efforts either to enter the market with substitute products or to introduce superior technologies.[33] In other instances, the owner of an upstream platform can achieve proprietary control over significant swathes of downstream markets by rendering the platform interoperable only with its own or its licensees' downstream goods and services.[34] The monopolists' redesign of their products can then enable them to vertically integrate, and thus eliminate their downstream competitors.[35] Although such integration is usually efficient,[36]

29. *See, e.g.*, Frank H. Easterbrook, *The Chicago School and Exclusionary Conduct*, 31 HARV. J.L. & PUB. POL'Y 439, 440 (2008) (observing that "[a]ntitrust law and bankruptcy law go hand in hand"); Hovenkamp, *supra* note 25, at 24.

30. *Cf.* Lee Goldman, *The World's Best Article on Competitor Suits for False Advertising*, 45 FLA. L. REV. 487, 505 (1993) (noting that "competitors have no incentive to bring" lawsuits where the practice has had "little impact on any individual competitor").

31. *See, e.g.*, Jonathan Jacobson, Scott Sher & Edward Holman, *Predatory Innovation: An Analysis of* Allied Orthopedic v. Tyco *in the Context of Section 2 Jurisprudence*, 23 LOY. CONSUMER L. REV. 1, 27 (2010) (opining that "[i]nnovation through redesign can marginally improve a product, but with overriding damage to the competitive process").

32. *See, e.g.*, Nicholas Economides & William N. Hebert, *Patents and Antitrust: Application to Adjacent Markets*, 6 J. ON TELECOMM. & HIGH TECH. L. 455, 480 (2008).

33. *See, e.g.*, *id.*

34. *See, e.g.*, Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1617 (2002).

35. *See, e.g.*, Dennis W. Carlton, *Economic Analysis of Antitrust Issues Raised by E-Commerce*, 1236 PLI/CORP. 121, 174 (2001).

and hence desirable, it may sometimes yield anticompetitive exclusionary effects.[37]

In theory then, a nonexistent or insignificant "improvement" can delay or eliminate the onset of competition, reducing levels of static efficiency without a concomitant and offsetting dynamic-efficiency gain.[38] Theoretical risks, though, do not necessarily beget actual anticompetitive outcomes. In most cases, consumers' ability to make qualitative comparisons, inventors' incentives to maximize profit, and opportunities for third-party technological development render claims of predatory innovation highly suspect.[39] Nevertheless, in those limited cases where dominant companies can strategically innovate to harm competition, antitrust condemnation should presumably follow.[40] In practice, however, identifying genuine instances of anticompetitive exclusion presents a number of intractable difficulties.[41] As this Article argues, these challenges are often preclusive, which necessitates the law's permitting at least some acts of anticompetitive innovation to go unaddressed.

B. THE COURTS' UNSATISFACTORY ANALYSIS OF PREDATORY-INNOVATION CLAIMS

In the past fifteen years, three circuit courts of appeals have announced three very different standards for analyzing claims of predatory innovation. All three are unsatisfactory, though for different reasons. One approach permits the dominant firm to introduce any new product that constitutes an "improvement" of its earlier version.[42] The second applies a fully fledged balancing test to determine whether or not a new product is predatory.[43] The third looks to consumers' response to the new product: if consumers preferred it to the product's predecessor, there is no predatory effect.[44] The

36. *See, e.g.*, James C. Cooper et al., *Vertical Antitrust Policy as a Problem of Inference*, 23 INT'L J. INDUS. ORG. 639, 658 (2005); *see also* Andy C.M. Chen & Keith N. Hylton, *Procompetitive Theories of Vertical Control*, 50 HASTINGS L.J. 573, 575–80 (1999).

37. *See, e.g.*, Steven C. Salop & David T. Scheffman, *Raising Rivals' Costs*, 73 AM. ECON. REV. 267, 267 (1983); *see also* Richard A. Posner, *Vertical Restraints and Antitrust Policy*, 72 U. CHI. L. REV. 229, 229–30 (2005).

38. *See, e.g.*, Janusz A. Ordover, Alan O. Sykes & Robert D. Willig, *Predatory Systems Rivalry: A Reply*, 83 COLUM. L. REV. 1150, 1151 (1983).

39. *See* Joseph Gregory Sidak, *Debunking Predatory Innovation*, 83 COLUM. L. REV. 1121 (1983).

40. *See* Easterbrook, *supra* note 29, at 443.

41. *See id.*

42. Allied Orthopedic Appliances, Inc. v. Tyco Health Care Grp., 592 F.3d 991, 998–99 (9th Cir. 2010).

43. United States v. Microsoft Corp., 253 F.3d 34, 59 (D.C. Cir. 2001).

44. C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340 (Fed. Cir. 1998).

following pages discuss each of these approaches, explaining their respective limitations and using them to illustrate the difficulty of crafting effective antitrust rules to govern claims of exclusionary invention.

1. The Ninth Circuit's Normatively Incomplete Rule: Minimally Significant Improvement as a Bar to Antitrust Liability

The Ninth Circuit is the most recent federal appellate court to grapple with the difficult antitrust questions that claims of predatory invention implicate. In *Allied Orthopedic Appliances, Inc. v. Tyco Health Care Group*,[45] a group of hospitals and other health care providers alleged, among other things, that Tyco held a dominant position in the pulse-oximetry market—the market for sensors and monitors that read and display a patient's level of blood oxygenation.[46] Plaintiffs asserted that Tyco's dominance arose in significant part from a patent on its technology and that, when the relevant patent expired, generic sensors compatible with Tyco's monitors would quickly enter the market and erode Tyco's dominance.[47] In anticipation of that prospect, plaintiffs alleged, Tyco developed and marketed new, patented monitors and sensors that employed new and more efficient features that were incompatible with generic sensors.[48]

Plaintiffs claimed that, by acting in the manner described above, Tyco had unlawfully maintained its monopoly power through the "predatory" redesign of its sensors and monitors, in violation of Section Two of the Sherman Act.[49] The Ninth Circuit rejected that claim, affirming the district court's ruling that Tyco's design change was not predatory. The court held more generally that a dominant firm's design change that improves its flagship product in some way and is not associated with separate anticompetitive conduct does not violate Section Two.[50] In reaching this conclusion, the court rejected plaintiffs' argument that the proper standard should weigh the benefits of product redesign against its anticompetitive effects, and it thus declined to adopt the D.C. Circuit's multi-factor balancing approach,[51] discussed in Section II.B.2, *infra*. Any such test, the Ninth Circuit concluded, would pose serious problems of judicial administration and doctrinal coherence.[52]

45. 592 F.3d 991.
46. *Id.* at 994.
47. *Id.* at 1001.
48. *Id.* at 995.
49. *Id.* at 1002.
50. *Id.* at 998–1003.
51. *Id.* at 1000.
52. *Id.* at 998–1000.

As to Tyco's change in design, the court pointed to undisputed evidence that the change was an unequivocal "improvement" as the new sensors provided more efficient calibration than their predecessors. The court also placed significant weight on the fact that the PTO had granted Tyco a patent on the new sensors.[53] In response to plaintiffs' argument that their evidence indicated that Tyco had hoped its redesign would forestall generic entry, the court held "[s]tatements of an innovator's intent to harm a competitor through genuine product improvement are insufficient by themselves to create a jury question under Section [Two]."[54] Finally, the court found that Tyco had not used its market power to force consumers to purchase its new sensors and monitors.[55] Although Tyco discontinued its previous line of monitors, the court observed, other monitor makers were competing in the relevant market.[56]

Although the court was right to conclude that improving a product should not give rise to an antitrust claim, the Ninth Circuit's analysis leaves unresolved several issues at the core of predatory-innovation claims. Most obviously, although it purported to eschew any formal calculus as to the net welfare gains of the relevant innovation, the court based its analysis on the conceded fact that the design change was superior.[57] Yet, many future cases are bound to entail disputes about the genuineness and extent of any proclaimed invention. In circumstances where the fact and degree of a purported improvement are debatable, the court provided no guidance, implicit or otherwise, as to whether the requisite antitrust analysis would be different.

Second, consumers' ability to reveal their preference for the improved product vis-à-vis the rivals' competing goods was central to the Ninth Circuit's ruling.[58] As the alleged instance of predatory innovation did not deprive consumers of freedom of choice, the market could act as a credible (perhaps dispositive) arbiter of qualitative improvement. Tyco's competitors remained free to market alternative, albeit non-infringing, monitors, leaving market processes and consumer choice intact. Given the presence of post-improvement competition, the court did not need to confront the question of what the result would have been if Tyco had withdrawn its earlier products from the market, leaving consumers with less, or no, choice of

53. *Id.* at 1000–01.
54. *Id.* at 1001.
55. *Id.* at 1002.
56. *Id.*
57. *Id.* at 994.
58. *See id.*

alternatives, or the question of whether that withdrawal would constitute the separate anticompetitive act required by its test.

A third issue concerns the role of the PTO. The determination by an expert administrative agency that the claimed invention deserved a twenty-year exclusive right on account of its novelty, utility, and non-obviousness would strike many observers as noteworthy.[59] In the quest to evaluate the quality of invention for antitrust purposes, however, should this fact be dispositive or simply relevant?[60] Might it conceivably be immaterial in light of the PTO's low threshold for utility?[61] The Ninth Circuit thought it worthy of consideration.[62] Indeed, the first piece of evidence that it considered in determining the fact and quality of invention was "the existence of a patent on a new product design."[63] The court concluded that it was "evidence that the change [was] an improvement over previous designs."[64] Since, however, a product change that is arguably novel and useful in satisfaction of the Patent Act might not necessarily "improve" the product, courts might need to assess the fact of improvement without regard to the issuance of a patent for the change.

2. The D.C. Circuit's Unworkable Balancing Test

By forgoing a balancing test in favor of a more definitive approach, the Ninth Circuit implicitly rejected the analysis of the U.S. Court of Appeals for the District of Columbia Circuit in *United States v. Microsoft Corp.*[65] One of the claims in that case was that Microsoft's integration of its Internet Explorer web browser with its operating system constituted a predatory design change intended to afford it monopoly power in the browser market and thus enable it to remain dominant in the market for PC operating systems.[66] The plaintiff alleged three separate ways in which the integration was predatory, and the D.C. Circuit analyzed each of those allegations pursuant to a balancing test of its own making.

---

59. *See* 35 U.S.C. §§ 101–103 (2010).

60. *See, e.g.*, Peter M. Boyle, Penelope M. Lister & J. Clayton Everett, Jr., *Antitrust Law at the Federal Circuit: Red Light or Green Light at the IP-Antitrust Intersection?*, 69 ANTITRUST L.J. 739, 797 (2002) ("The notion that the patent laws confer some affirmative right to modify patented products, thereby implicitly exempting patentees from antitrust liability for predatory product modifications, makes little sense given the nature of the patent right.").

61. *See, e.g.*, M. Scott McBride, Note, *Patentability of Human Genes: Our Patent System Can Address the Issues Without Modification*, 85 MARQ. L. REV. 511, 523 (2001) (observing that "the utility requirement appears to be minimal").

62. *Tyco*, 592 F.3d at 1000–01.

63. *Id.*

64. *Id.*

65. 253 F.3d 34, 59 (D.C. Cir. 2001).

66. *Id.* at 65–67.

Before applying its test, the panel observed that courts generally ought to be "very skeptical about claims that competition has been harmed by a dominant firm's product design changes," and that, in rapidly changing markets, skepticism was especially warranted.[67] On the other hand, it noted, skepticism about these kinds of claims should not amount to a per se rule of legality for all such changes.[68] The D.C. Circuit concluded that the proper approach would consist of a three-part test: first, the plaintiffs would need to show that the design changes in question resulted in anticompetitive effects; if they made such a showing, the defendants would then have to demonstrate that those changes produced procompetitive effects.[69] If the defendants did so, then the plaintiffs would bear the ultimate burden of demonstrating that the proven anticompetitive effects outweighed the proven procompetitive ones.[70]

The application of that test in *Microsoft* was remarkably—and uncommonly, one might think—simple. For two of the challenged changes, Microsoft offered no procompetitive justification; and, for the third, plaintiff failed to rebut Microsoft's procompetitive justification.[71] Consequently, the court never reached the point where it needed to balance conflicting effects. One might imagine any number of plausible scenarios, however, in which the parties submit conflicting evidence as to the competitive effects of a dominant firm's impugned invention. The D.C. Circuit offered no particulars as to how its balancing calculus would operate. Nor are the mechanics for applying such a test in any way obvious. The candidates for consideration—the short-term harms and long-term benefits, both qualitative and quantitative, occasioned by an invention—are either incommensurable or incomparable, or both.[72] Even if judges could articulate a logical framework within which to carry out this utilitarian calculation—which would itself be an heroic feat—it would be difficult, if not impossible, to guide juries through the test in a coherent way. That problem, in turn, might result in courts making decisions on the basis of their perceptions of the technical merits of the change in question.

Identifying the "merits" of a new technology, however, constitutes the single most intractable aspect of the law governing both anticompetitive

67. *Id.* at 64–65.
68. *Id.* at 65.
69. *Id.* at 58–59.
70. *Id.*
71. *Id.* at 66–67.
72. These factors are incommensurable because courts have little ability to determine the long-run impact of a new product design or other innovation on consumer welfare and thus cannot reliably include such considerations in a calculus to determine whether the net impact of a challenged invention is positive.

innovation generally, and the D.C. Circuit's balancing test specifically. The question whether a purported improvement is indeed what it claims to be is of inescapable importance to antitrust analysis, but its resolution is problematic. The principal difficulty is one of definition. In other words, do technological benefits, presumably as evidenced (and disputed) by expert testimony from scientists and engineers, control the fact and quality of invention? Or do consumer purchases—themselves potentially subject to distortion-inducing biases or bouts of irrationality—constitute the final word?

A second, closely related problem involves the source and nature of proof. Although competition law traditionally places heavy weight on consumer choice,[73] market processes may be imperfect indicators of consumer demand in a less-than-fully informed world.[74] By the same token, though, expert testimony about the intricacies of a particular technology may likewise produce inaccurate conclusions. Even if a "correct" answer exists as to the merits of a technological improvement, expert evidence may not be an effective guide to judicial decision making. Numerous studies have questioned the utility of expert testimony when the determination of truth lies with lay judges or jurors, who are prone to reach arbitrary conclusions in technologically complex cases.[75] In other contexts, the new product may display subjective qualities—such as its "look" or "feel"—that preclude universal, or objectively falsifiable, scientific conclusions as to whether the relevant change is desirable, neutral, or unwelcome. This might be most likely in cases of incremental changes in product design, which are ubiquitous in the modern economy.[76] In the absence of a verifiable answer to the question whether an innovation is beneficial, how can courts attempt to weigh its magnitude against an alleged harm to competition?

If the D.C. Circuit was indeed "very skeptical" of claims of predatory innovation,[77] its skepticism must have reflected the view that evidence of predation accompanying most allegations of anticompetitive innovation is unconvincing. Such a prediction, however, does nothing to aid analysis. Moreover, the standard that the D.C. Circuit devised took little account of the skeptical view upon which the court professed to base its analysis. If product design is almost invariably desirable and only in exceptional cases

73. *See, e.g.*, Nat'l Collegiate Athletic Ass'n v. Bd. of Regents of Univ. of Okla., 468 U.S. 85, 102 (1984).

74. *See infra* Section II.B.4.

75. *See, e.g.*, Scott Brewer, *Scientific Expert Testimony and Intellectual Due Process*, 107 YALE L.J. 1535, 1539 (1998).

76. *See, e.g.*, Michael J. Burstein, *Rules for Patents*, 52 WM. & MARY L. REV. 1747, 1769 (2011).

77. United States v. Microsoft Corp., 253 F.3d 34, 65 (D.C. Cir. 2001).

predatory, as the D.C. Circuit implicitly recognized,[78] then the law should entertain antitrust claims founded on exclusionary innovation with a healthy dose of doubt. In fashioning a rule for addressing claims of predatory innovation, however, the court enunciated a standard free from ingrained or systemic bias against such claims.[79] Beyond putting the initial burden of proof on the plaintiff—an allocation common to all civil cases[80]—the D.C. Circuit's test created an analytic framework equally conducive to findings of legality and illegality.

This neutral approach is problematic. Courts in monopolization cases must rely on unquantifiable and probabilistic long-term effects. Since short-run anticompetitive effects are easier to assess and are more available, a neutral test will systematically overweigh them at the expense of a fair assessment of long-term benefits. Indeed, it is easier to demonstrate some "harm" to competition in the short-run, static sense than it is to disprove anticompetitive consequences by appealing to economic theory governing dynamic effects.[81]

3. The Federal Circuit's Illogical Approach: Establishing Predatory Innovation Through Intent

The single most ill-conceived treatment of predatory innovation arose in the 1998 case *C.R. Bard, Inc. v. M3 Systems, Inc.*[82] In response to a patent infringement lawsuit brought against it, the defendant, M3 Systems, filed an antitrust counterclaim asserting that the plaintiff, C.R. Bard, had modified its patented product specifically to render it incompatible with competitors' complementary parts.[83]

The patented good in question was Bard's "Biopty gun"—a mechanical device for extracting human tissue samples—which went through three iterations.[84] The first version, which required the simultaneous efforts of two physicians to operate, fired a particular brand of biopsy needle, "Tru-Cut," into the target tissue.[85] Three years later, the inventor sought to improve the

78. *Id.*

79. *Id.* at 58–59.

80. *See, e.g.*, Amy Dieterich, *The Role of the State Attorney General in Preventing and Punishing Hate Crimes Through Civil Prosecution: Positive Experiences and Possible First Amendment Potholes*, 61 ME. L. REV. 521, 526 (2009).

81. For the authors' larger discussion of this issue, see Michael Jacobs & Alan Devlin, *The Riddle Underlying Refusal-To-Deal Theory*, 105 NW. U. L. REV. 1 (2010).

82. 157 F.3d 1340 (Fed. Cir. 1998).

83. *Id.* at 1346.

84. *Id.* at 1346–48.

85. *Id.* at 1347.

operation of the gun by redesigning it so that users would not have "to cock the two drivers manually before installing the biopsy needles, a step described as awkward and inefficient."[86] The second-generation gun entailed the use of a ring that allowed a single user to cock the drivers after he had placed the needles in the gun.[87] Since the Tru-Cut needles could not move both forward and backward, a feature supposedly necessary to the improved gun's operation, they were incompatible with the second version.[88] The third, and final, iteration reduced the manual force needed to cock the driver springs through an external mechanism that energized the two springs separately. The inventor obtained additional improvement patents for both the second- and third-generation guns.[89] Bard subsequently acquired these intellectual property rights. M3, which Bard accused of infringing those patents, alleged that Bard had deliberately modified its biopsy gun so that it would not work with Tru-Cut needles.[90]

A divided Federal Circuit upheld a jury verdict of attempted monopolization, based on evidence that the desire to exclude manufacturers of replacement needles motivated Bard to modify its gun.[91] The majority articulated an intent-based test for evaluating the legality of a product-design change, holding that "M3 was required to prove that Bard made a change in its Biopty gun for predatory reasons, i.e., for the purpose of injuring competitors in the replacement needle market, rather than to improve the operation of the gun."[92] The majority pointed to, among other things, two internal Bard documents that arguably suggested that the modifications were devoid of technological merit.[93] The obvious perversity underlying this standard is that it substitutes subjective intent for market-based analysis that would calculate the actual price and innovation effects of a challenged form of innovation.[94]

The court's holding invited a sharp dissent from Judge Newman. She opined:

> Both the needle assembly alone and the integrated biopsy gun/needle device were patented. They were subject to Bard's

86. *Id.*
87. *Id.*
88. *Id.* at 1376.
89. *Id.* at 1347–48.
90. *Id.* at 1369.
91. *Id.* at 1382.
92. *Id.*
93. *Id.*
94. *See, e.g.*, Ball Mem'l Hosp., Inc. v. Mutual Hosp. Ins., Inc., 784 F.2d 1325, 1339 (7th Cir. 1986) ("Vigorous competitors intend to harm rivals, to do all the business if they can. To penalize this intent is to penalize competition.").

> patent-based rights to exclude others from making, using, or selling them. It was not Bard's changes to its biopsy gun or needles that affected M3's sale of replacement needles; it was the patents on these products. To hold that Bard could violate the Sherman Act by changing these products, if M3's business was adversely affected, is a novel and pernicious theory of antitrust law that is contrary to the principles of competition, and fraught with litigation-generating mischief.
>
> . . . .
>
> . . . It is without precedent to find antitrust liability premised on a theory that development of new products is illegally anticompetitive when the new product requires competing suppliers to adjust their product accordingly. . . . If this court deems it appropriate to add this burden to patent-based innovation, there should at least be some overriding public benefit. However, antitrust jurisprudence has well understood that the enforcement of the antitrust laws is self-defeating if it chills or stifles innovation.[95]

Judge Newman's dissent reflects the consensus of opinion among antitrust scholars and judges well versed in antitrust law that the law is meant to protect competition, not competitors. Real innovation fosters competition—and is often the essence of competition—because it requires competitors of the innovating firm to invent and develop their own improvements if they wish to survive, a requirement that redounds strongly to the benefit of consumers.

As explained in more detail in the Section III.B, *infra*, subjective intent is often a red herring in antitrust analysis and ought to be irrelevant in these cases. Ultimately, the Federal Circuit's holding rested on a flimsy rationale. Beyond the criticisms articulated by Judge Newman and the court's imprudent focus on subjective intent, the challenged product design wrought no economic harm. By excluding M3's and other competitors' needles from use in operation with its gun, Bard integrated vertically. Although there are circumstances in which such integration can injure consumers,[96] the process is generally efficient, as it was in the case of *C.R. Bard*. Economic analysis demonstrates that vertical integration is desirable when the upstream manufacturer can supply downstream or complementary products or services

95. *C.R. Bard*, 157 F.3d at 1370–72 (Newman, J., dissenting) (citations omitted).
96. *See* Posner, *supra* note 37, at 240–41.

at a lower cost than third parties can supply such products.[97] By eliminating the Cournot-complements problem,[98] vertical integration can generate higher output and lower prices.[99] This benefit was lost on the majority, likely because it substituted "intent" for economic analysis.

4. *The Second Circuit's Problematic Test: Consumer Preference as a Conclusive Determinant of Legality*

Even before the articulation of the tests described above, the Second Circuit had devised a test of its own in the well-known case of *Berkey Photo, Inc. v. Eastman Kodak Co.*[100] That litigation arose after Kodak—the then-dominant firm in markets for film, color-print paper, and cameras—introduced a new pocket camera along with a new film designed to produce clear-color prints from smaller negatives, but through a new photofinishing process that was incompatible with the process previously in use.[101] The new products were popular with consumers, but Berkey, unaware of the pocket camera's imminent introduction, could offer nothing to compete with Kodak for some months after the Kodak camera came to the market.[102] This allegedly placed Berkey at a severe competitive disadvantage.[103] Among other claims, Berkey argued that the product introduction was predatory because the new film was not an improvement over existing kinds, and also because the combination of the new film and new photofinishing process was unnecessary to produce good photographs with the new camera.[104]

Rejecting Berkey's claims, the court first recited the well-accepted principle that as a general matter "any firm, even a monopolist, may . . . bring its products to market whenever and however it chooses."[105] This did not mean, the court added, that new product introductions were immune from

97. *See* Herbert Hovenkamp, *Vertical Integration by the Newspaper Monopolist*, 69 IOWA L. REV. 451, 464 (1984); *see also* J. Gregory Sidak, *A Consumer-Welfare Approach to Network Neutrality Regulation of the Internet*, 2 J. COMPETITION L. & ECON. 349, 459 (2006).

98. A Cournot-complements problem arises when two separate entities have respective monopolies over two separate products that one must combine to create a final product. A negative externality afflicts the relevant pricing decisions because each owner fails to take into account the fact that decreasing the price of one complementary good would increase demand for the other product. If the two products come under common ownership, these effects will be internalized and efficient pricing decisions will result.

99. *See, e.g.*, Randall Heeb, *Innovation and Vertical Integration in Complementary Markets*, 12 J. ECON. & MGMT. STRATEGY 387 (2003).

100. 603 F.2d 263 (2d Cir. 1979).

101. *Id.* at 267–71.

102. *Id.* at 269.

103. *Id.*

104. *Id.* at 283–86.

105. *Id.* at 286.

antitrust scrutiny, but rather that any antitrust violation must come not from "the product introduction itself, but [from] some associated conduct."[106] The court then observed, in what seemed to be the distillation of its test, that "[i]f a monopolist's [new] products gain acceptance in the market, . . . it is of no importance that a judge or jury may later regard them as inferior, so long as that success was not based on any form of coercion."[107] As it could find no evidence that Kodak had coerced consumers into purchasing the new camera system, the court held that the product introduction was not anticompetitive.[108]

The Second Circuit's approach is a consumer-preference test with a twist. If consumers like the new product—regardless of its technical merits (i.e., whether and how much it represents an improvement)—then there is no predation. If they dislike the new product, then it makes no difference whether the product is "predatory," since rivals have suffered no harm on account of its introduction and therefore lack standing to sue. This test puts primacy of place on consumer autonomy, allowing individual purchasers to effectively determine legality by signaling their preferences through the market. It evaluates the "quality" of an improvement democratically, by resort to a consumer referendum, without regard to technical proof of the scientific merit underlying the new product. One might say that the consumer-preference test reflects a libertarian perspective, even allowing people irrationally to elect technologically inferior products or higher-priced goods that are not "truly" innovative. This perspective would decline to deploy antitrust, or any other body of law, to prevent any firm, even a dominant one, from marketing goods that consumers desire but would shun if they knew better.

The twist—common perhaps to *Tyco*, *Microsoft*, and *Berkey*—lies in the concept of "coercion." As a general matter, this qualification makes eminent sense because consumers cannot demonstrate their relative tastes for a new product when a company deprives them of choice. Thus, by its own terms, the consumer-preference test would seem inapplicable to cases in which a dominant company's allegedly predatory improvement prevents any third party from marketing a rival product. An ordinal ranking of products in a market that consists of a single good does not convey any useful information as to the qualitative characteristics of that product. Simply put, consumer preference cannot emerge when the consumer's choice is a take-it-or-leave-it proposition.

106. *Id.* at 286 n.30.
107. *Id.* at 287.
108. *Id.* at 287–88.

While this is an important limitation on the Second Circuit's test, its meaning is inevitably unclear. The concept of "coercion" encapsulates restrictions of varying severity. When strategic marketing of new goods precludes the availability of substitutes, as in certain instances of product hopping discussed in Part V, *infra*, "coercion" clearly exists. Yet, an allegedly improved product, introduced by a dominant firm, may enjoy scale, marketing, network effects, and other benefits independent of technological merit that partially constrain consumer choice. Where market processes are corrupted, but not entirely inoperative, consumer purchases, though indicative, may be a misleading guide to the technological merits of the challenged product. Indeed, in its purest form, the "coercion" limb of the consumer-choice test might regard any material advantage enjoyed by the seller of the "improved" product as capable of corrupting consumer choice and thus undermining the signaling value of market sales. In short, because consumer free will is an abstraction, the *Berkey* test, though linguistically pleasing, is both incomplete and problematic in practice.

C. MEASURING THE QUALITY OF INVENTION

The preceding cases illustrate a panoply of difficult legal issues implicated by antitrust oversight of technological advancement. The chief problem involves measuring the quality of an assailed invention. After all, if courts ex post and companies ex ante could both reliably and cheaply determine which claimed improvements are illusory, no policy dilemma would accompany claims of predatory innovation. Unfortunately, a variety of constraints prevent such a felicitous outcome. In light of courts' fact-finding limitations and inventors' imperfect ability to predict judicial conclusions about the legality of their behavior, how should antitrust law treat claims of innovation-based monopolization?

The decisions discussed above demonstrate how the courts have thus far answered this question. Those decisions reflect contrasting levels of confidence in the judiciary's self-assessed ability to conduct antitrust oversight of technology in a reliable and effective manner. Given the serious practical constraints on judges' and juries' capacity for determining the scientific or engineering merit of an assailed innovation ex post, the Second Circuit favors treating consumer demand for an improved product, absent coercion, as conclusive evidence of quality.[109] Similarly skeptical about its ability to quantify the significance of a purported improvement, the Ninth Circuit deems a finding of *some* advance to be inconsistent with an antitrust

109. *Id.*

violation.[110] Uniquely sanguine about its ability to engage in an invention-specific, utilitarian cost-benefit analysis, the D.C. Circuit advocates a balancing test that weighs the magnitude of an improvement against its exclusionary effect.[111] Whether its faith is justified is an open matter, for—it bears emphasizing—the court did not even have occasion to apply the rule that it championed. Furthermore, in the Federal Circuit, the quality of a purported improvement is irrelevant: real innovation "intended" to harm rivals is subject to condemnation even when it is socially beneficial.[112]

In our view, antitrust oversight of innovation is fraught with danger. The pace and complexity of technological advancement in the new economy far exceed the capabilities of the judicial process to identify and assess bona fide invention accurately. The principal problems with competition law's review of dominant-firm innovation are three-fold. First, the glacial pace of litigation renders antitrust enforcement largely ineffective in constraining even genuine acts of predatory innovation.[113] Monopolization cases invariably span many years, during which time scientific progress may well have rendered the technology at issue obsolete.[114] Even putting error costs aside, the expense of prosecuting and defending antitrust cases is hard to justify when the real effect of such enforcement actions is irrelevant.

Second, assuming that the impugned invention remains commercially significant upon resolution of antitrust proceedings, the limited remedies available to a court preclude effective correction of distorted market conditions.[115] Prior monopolization cases make competition law's remedial deficiencies painfully apparent, revealing that antitrust remedies are no

110. Allied Orthopedic Appliances, Inc. v. Tyco Health Care Grp., 592 F.3d 991, 998–99 (9th Cir. 2010).

111. United States v. Microsoft Corp., 253 F.3d 34, 58–59 (D.C. Cir. 2001).

112. C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340, 1382 (Fed. Cir. 1998).

113. *See, e.g.*, Lee Goldman, *Oligopoly Policy and the* Ethyl Corp. *Case*, 65 OR. L. REV. 73, 93–94 (1986); *see also* Dan G. Barry, Comment, *The Effect of Video Franchising Reform on Net Neutrality: Does the Beginning of IP Convergence Mean That It Is Time for Net Neutrality Regulation?*, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 421, 436 (2008).

114. *See, e.g.*, David J. Teece & Mary Coleman, *The Meaning of Monopoly: Antitrust Analysis in High-Technology Industries*, 43 ANTITRUST BULL. 801 (1998); *see also* Mika Kato, *Transitoriness of Market Power and Antitrust Activity*, 6 J. COMPETITION L. & ECON. 393, 395–96 (2010). *But see* Michael A. Carrier, *Pictures at the New Economy Exhibition: Why the Antitrust Modernization Commission Got It (Mostly) Right*, 38 RUTGERS L.J. 473, 475 (2007).

115. *See, e.g.*, Jonathan B. Baker, *Preserving a Political Bargain: The Political Economy of the Non-interventionist Challenge to Monopolization Enforcement*, 76 ANTITRUST L.J. 605, 617 (2010) (summarizing the Chicago School view as to why monopolization enforcement is likely to be ineffective and counterproductive); Einer Elhauge, *Disgorgement as an Antitrust Remedy*, 76 ANTITRUST L.J. 79, 87 (2009); John E. Lopatka, *Assessing Microsoft from a Distance*, 75 ANTITRUST L.J. 811, 813–14 (2009).

substitute for free-market forces generally, and third-party innovation in particular.[116] By far the most prominent new-economy antitrust case against predatory innovation was *Microsoft*.[117] That litigation spanned nearly a decade,[118] and despite a harsh consent decree that imposed certain interoperability requirements and otherwise sought to dilute the operating system monopoly, economists regard the remedies as an abject failure.[119] The consent decree came to a close in 2011 without much notice.[120]

Crucially, technology-based competition from Google and Apple, among others, has eviscerated Microsoft's dominance, which was commonly supposed to be unassailable only a few years before.[121] A recent feature in *The Economist* observed that Microsoft's future looks uniquely vulnerable vis-à-vis those of its closest rivals.[122] Perhaps most remarkably, the company has recently joined the chorus of self-proclaimed victims of anticompetitive practices, adding its voice to those criticizing the new successful innovator on the block, Google.[123] This is itself a stunning indictment of the antitrust system, revealing its proclivity to become a vehicle for failing competitors to seek recourse through competition laws.

Third and most importantly, ex post judicial scrutiny of innovation is an inexact science that defies reliable application.[124] Courts faced with a challenge to a new product must answer four very difficult questions: Has there been an "innovation" to the relevant product, or simply a "change"? If there has been an innovation, how significant must it be, on a scale ranging

116. *See* Lopatka, *supra* note 115, at 813–14.

117. *See* discussion *supra* Section II.B.2.

118. Christian Ahlborn & David S. Evans, *The Microsoft Judgment and Its Implications for Competition Policy Towards Dominant Firms in Europe*, 75 ANTITRUST L.J. 887, 888 (2009).

119. *See* Robert W. Crandall & Charles L. Jackson, *Antitrust in High-Tech Industries*, TECH. POL'Y INST. (Dec. 2010), http://techpolicyinstitute.org/files/crandalljackson%20antitrust_in_high_tech3.pdf.

120. *See, e.g.*, Bianca Bosker, *Microsoft's Antitrust Saga Finally Comes to an End*, HUFFINGTON POST (May 25, 2011), http://www.huffingtonpost.com/2011/05/12/microsofts-antitrust-saga_n_861281.html; Jay Greene, *Microsoft Oversight Ends with Little To Show for Effort*, CNET NEWS (May 12, 2011), http://news.cnet.com/8301-10805_3-20062079-75.html.

121. *See* Robert Cyran & Martin Hutchinson, *At Microsoft, Bing Too Costly To Keep*, N.Y. TIMES, July 25, 2011, at B2; Elizabeth Flock & Hayley Tsukayama, *Apple Announces Free iCloud Service*, WASH. POST, June 7, 2011, at A10; Opinion, *Remember Microsoft?*, N.Y. TIMES, June 11, 2011, at A20; Martin Peers, *A Window into Microsoft's Profit Outlook*, WALL ST. J., Mar. 20, 2010, at B16; Seth Schiesel, *Game Changer*, N.Y. TIMES, June 9, 2011, at F1.

122. *Microsoft: Middle-Aged Blues*, ECONOMIST, June 13, 2011, at 12; *see also IBM: 1100100 and Counting*, ECONOMIST, June 13, 2011, at 11.

123. *See* Steve Lohr, *Antitrust Cry from Microsoft*, N.Y. TIMES, Mar. 31, 2011, at B1.

124. *See, e.g.*, Marina Lao, *Reclaiming a Role for Intent Evidence in Monopolization Analysis*, 54 AM. U. L. REV. 151, 179–86 (2004).

from "trivial" to "transformative"? Once the criteria for measuring the magnitude of an innovation have been settled, how should they be assessed and by whom? And, finally, how are the benefits of the innovation to be compared with its harm to competition? In grappling with these questions, judges and juries are likely to err regularly. The price of false positives—erroneous findings that a social-welfare-increasing act of invention was welfare-decreasing—is likely to be severe.[125] Given the overriding importance of innovation to the economy, legal standards that threaten to punish a dominant firm for introducing new technology can have damaging repercussions.[126]

Nor are such problems unique to mistaken factual determinations. Improperly calibrated antitrust standards that leave inventors uncertain about the probable legality of their actions can depress innovative activity ex ante. The second-order effects of mistaken antitrust analysis of exclusionary invention are serious. Yet, total deference to the marketing of dominant firms' self-proclaimed improvements, with no antitrust enforcement, could conceivably foreclose channels for follow-on innovation, thus denying consumers competing sources of technological development and commercialization.

These three features at the intersection between antitrust and innovation demonstrate the dangers attendant upon applying the former to the latter. The following two Parts articulate our view on the optimal antitrust rules governing claims of technology-based predation. Part V then applies this proposed framework to what many consider to be the single most blatant act of predatory innovation, "product hopping" in the pharmaceutical industry. Contrary to prevailing academic opinion, we conclude that strategic manipulation of the pharmaceutical regulatory structure generally lies outside of antitrust law's remit. We thus urge, for the most part, a regulatory or legislative solution to the problem in lieu of a judicial one. Only where a hop successfully forecloses entry should antitrust law intervene.

III. AN ANALYTIC FRAMEWORK FOR ADDRESSING CLAIMS OF PREDATORY INNOVATION

As the preceding discussion explained, in assessing claims of predatory innovation, the courts have adopted inconsistent and inadequate rules for

125. *See, e.g.*, Geoffrey A. Manne & Joshua D. Wright, *Google and the Limits of Antitrust: The Case Against the Case Against Google*, 34 HARV. J.L. & PUB. POL'Y 171, 182–84 (2011).

126. *See, e.g.*, *id.*

analyzing the fact and extent of innovation by the dominant firm and for determining the competitive effects of such innovation.

This Part identifies three factors that the law should ignore, even though they may appear to shed light on the question of whether a product design is predatory. The first factor would regard the PTO's decision to grant a patent over a claimed product or process as conclusive proof that the patented technology represents an improvement over the prior art. The second would use evidence of a defendant's intent to exclude a rival as a proxy for the lack of technological merit in the assailed invention. And the third would equate the presence of "coercion" with consumer harm and find an antitrust violation on that basis. Far from being helpful guides to analysis, these factors are rarely relevant, and often misleading, when applied to claims of alleged monopolization by innovation.

A. THE PTO

Should it be a complete defense for a company accused of predatory innovation that it possesses a patent over the challenged product design? This question implicates two distinct and important considerations. The first is whether the fact of patent issuance demonstrates a threshold level of qualitative improvement over the prior art. If it does, the consequences would be significant. In those jurisdictions that reject the possibility of an antitrust violation if the assailed product offers some genuine improvement—namely, the Ninth and Second Circuits[127]—the fact of patent protection would dispose of claims of predatory innovation. For jurisdictions that weigh the benefits of an invention against its costs to competition—specifically, the D.C. Circuit[128]—patent protection would be relevant to the net-welfare calculus. The second consideration is whether a patent necessarily precludes any role for antitrust analysis. If a patent amounts to a lawful monopoly, does it protect a dominant company from liability for any form of product-design-based exclusion?

Many might suppose that the issuance of a patent by the PTO conclusively disposes of the question of technological merit. An expert agency's decision to grant a twenty-year exclusive right over a new, useful, and nonobvious invention surely reflects a determination of scientific achievement worthy of deference.[129] A patent alone, however, is a poor proxy for the existence and magnitude of any innovation that may underlie a

127. *See supra* Sections II.B.1, II.B.4
128. *See supra* Section II.B.2.
129. *See* 35 U.S.C. §§ 101–103 (2010).

claimed invention.[130] To satisfy the utility requirement for patent issuance, an inventor need not establish that the claimed product or process is superior to the prior art; he need demonstrate only that it is operable to achieve a useful result.[131] The same holds true for so-called "improvement patents," which provide precious-little signaling value regarding the relevant qualitative enhancement incorporated within their claims.[132] To obtain such a patent, an inventor need only convince the PTO that the "improved" technology operates differently from the "basic" product or process.[133] For these reasons, courts should decline to presume that the existence of a patent over new technology marks that technology as inventive.

This does not mean of course that patented products or processes typically fail to advance the prior art. Some, perhaps many, entail significant improvements over the prior art. The point is that patent applications present the PTO with a spectrum of patentable inventions. At one end of the spectrum is what one might describe as an illusory act of invention, and at the other is the first wheel. In between lies a wide variety of qualitative improvements, some of which may be slight but valuable (for example, certain reformulations of drugs).

This observation leads to the second question, which is whether the fact of patent protection should shield all inventions from antitrust scrutiny, including those that lie at the "illusory" end of the spectrum. This question is complicated by the fact that the PTO may be simultaneously correct as a matter of patent law, as the invention satisfies the novelty and utility requirements, and incorrect as a matter of antitrust law, because it entails no material technological improvement and injures consumer welfare. Can antitrust laws correct, or disregard, a "mistaken" finding by the PTO, which enables a dominant firm to harm competition? This question implicates issues of comparative institutional competence, deference between conflicting fields of substantive law, and practical administration.

130. *See, e.g.*, Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989, 1007 n.78 (1997) (observing that "[t]he requirement that a patented invention be 'useful' is only laxly enforced" such that it is "possible to obtain a patent on a nonobvious but inefficient (relative to the prior art) way of doing things").

131. *In re* Swartz, 232 F.3d 862, 863 (Fed. Cir. 2000).

132. *See, e.g.*, Lemley, *supra* note 130, at 1007.

133. *See* 35 U.S.C. § 101 (allowing the inventor of "any new and useful improvement" to obtain a patent).

Taking the deference issue first, few question the sanctity of the patentee's right to exclude.[134] It is well established that patents are an "exception to the general rule against monopolies and to the right to access to a free and open market."[135] The antitrust laws generally have no application to a monopoly falling within intellectual property's sphere of exclusivity.[136] One might therefore conclude that a patent-covered invention, even one that represents no technological gain over the prior art, should enjoy absolute antitrust liability.[137] An argument in its favor might go as follows: If Congress saw fit to implement a patent system that grants a lawful monopoly to owners of inventions meeting certain statutory criteria, then a particular company's satisfaction of those criteria comports with patent law, and by extension, antitrust. Thus, if the PTO saw fit to bestow a patent on the relevant product's strategic alteration, the problem lies with the intellectual property laws and does not lend itself to an antitrust solution. A rule of per se legality, so justified, would also make sense from an administrative perspective because it would be simple to apply.

We disagree with this position. If a new product design represents a bona fide improvement, antitrust would and should welcome its introduction. But if a new design does not constitute an improvement over the replaced version and enjoys intellectual property protection, the patent might allow an anticompetitive use that would otherwise (with no patent) be impermissible. If the PTO is not determining utility, or if "utility" and "improvement" differ, then there seems to be no reason to defer to the PTO on the issue of "innovation."[138]

Refusing to deem a patent conclusive of a new product's legality under the antitrust laws does no violence to the sanctity of the intellectual property system. A patent constitutes a form of property, which confers on its owner certain rights. As is invariably the case in law, however, those rights are not

134. *See, e.g.*, Intergraph Corp. v. Intel Corp., 195 F.3d 1346, 1362 (Fed. Cir. 1999) (holding that "the antitrust laws do not negate the patentee's right to exclude others from patent property").

135. Walker Process Equip., Inc. v. Food Mach. & Chem. Corp., 382 U.S. 172, 177 (1965) (quoting Precision Instrument Mfg. Co. v. Auto. Maint. Mach. Co., 324 U.S. 806, 816 (1945)).

136. *See* Simpson v. United Oil Co. of Cal., 377 U.S. 13, 24 (1964) (finding that "the patent laws . . . are in pari materia with the antitrust laws and modify them pro tanto").

137. *See, e.g.*, C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340, 1370–72 (Fed. Cir. 1998) (Newman, J., dissenting).

138. Christopher R. Leslie, *Antitrust and Patent Law as Component Parts of Innovation Policy*, 34 J. CORP. L. 1259, 1285 (2009) ("Because patent holders may engage in conduct that improperly suppresses innovation, and patent law does not sufficiently constrain such behavior, decision makers who care about innovation should move toward antitrust.").

absolute but are rather contingent and qualified. A well-known set of antitrust limitations on a patentee's right to employ its property exists. These include so-called *Walker Process* fraud, in which patent applicants purposefully withhold information from the PTO that would preclude patentability;[139] patent-infringement proceedings where the patentee brings an objectively meritless lawsuit to enforce a patent that he knows to be invalid;[140] and the acquisition of patents from third parties to create an economic monopoly.[141] These limitations are consistent with patents' status as property, and the courts have acknowledged them. Representatively, the D.C. Circuit in *Microsoft* characterized as near "frivolous" the defendant's argument that it could not violate the Sherman Act by employing its lawfully granted property as it saw fit.[142] The court likened an inventor's possession of intellectual property to a person's wielding a baseball bat, pointing out that the latter would hardly enjoy immunity in using his property to attack a third party.[143]

Thus, in the context of predatory innovation, the ease of substituting one patent-protected good for another of immaterial technological distinction is such that the existence of intellectual property should not in itself foreclose an antitrust claim. To recognize an exemption from competition law in this instance would be improperly to confer a de facto right strategically to exclude equally or more efficient competitors under the guise of patent protection. As explained below, however, the circumstances in which the law should recognize a Sherman Act violation for exclusionary product design or other innovation are quite narrow. Specifically, where the relevant act of innovation does not prevent competitors' making their goods available to consumers, an antitrust claim of predatory invention should necessarily fail. Where a challenged product design actually forecloses rivals from the market, no antitrust violation should exist if the product entails a material improvement over the prior version. In determining whether such a material advance exists, the existence of a patent is by itself, not illuminative.

---

139. *Walker Process*, 382 U.S. 172.

140. *See, e.g.*, Deborah A. Coleman, *Antitrust Issues in the Litigation and Settlement of Infringement Claims*, 37 AKRON L. REV. 263, 273 (2004).

141. *See, e.g.*, United States v. Lever Bros. Co., 216 F. Supp. 887, 889 (S.D.N.Y. 1963). *See generally* John L. Murchison, *Patent Acquisitions and the Antitrust Laws*, 45 TEX. L. REV. 663 (1967).

142. United States v. Microsoft Corp., 253 F.3d 34, 63 (D.C. Cir. 2001).

143. *Id.* The accuracy of the court's analogy is questionable, given the many material differences between the economic principles that justify the recognition of rights in physical and intellectual property, respectively. Nevertheless, the D.C. Circuit was correct to reject the dogmatic view that antitrust imposes no constraint on the manner in which a patentee may exercise its exclusive rights.

B. INTENT

In *Microsoft*, the software giant conducted an all-out assault on Netscape's share of the Internet-browsing market with the self-described purpose of destroying its competitor.[144] In *C.R. Bard*, internal company documents revealed that the defendant had purposefully designed its biopsy gun to be incompatible with its rivals' needles, thus ensuring that complementary market for itself.[145] *Berkey* involved much-the-same circumstances as *C.R. Bard*, differing only in that the monopolized activity was photofinishing.[146] In *Tyco*, the defendant developed new medical sensors and monitors of limited technological improvement over the prior versions, presumably to prolong its period of dominance.[147]

In all of these cases, one need hardly be cynical to infer a selfish intent on the part of the innovating companies. Might such intent itself be "predatory," and therefore relevant to the legality of the challenged invention? Surely, the law should distinguish technological innovation that harms rivals as an indirect result of higher consumer demand for a superior product from strategic "improvements" that have as their explicit goal the destruction of competitors?[148] To grant dominant companies carte blanche strategically to market whatever kinds of insignificant improvements they choose is, from this perspective, to invite anticompetitive outcomes.

One might thus be tempted to summarily condemn predatory innovation of the kind described above. Monopolists' attempts to prolong or perpetuate their dominant position invariably run counter to short-term (static) competition and hence, one might suppose, undermine consumer welfare. Indeed, their efforts may operate in diametric opposition not only to antitrust's consumer-focused ideology, but also, in certain industries, to the goals of a relevant regulatory infrastructure intended to foster entry and lower prices.

Yet, identifying the optimal legal rules for assessing claims of exclusionary innovation is a far more complex matter than simply discerning the purpose behind a product-design change. Evidence of subjective

144. *Id.* at 76–77.

145. C.R. Bard, Inc. v. M3 Sys., Inc., 157 F.3d 1340, 1382 (Fed. Cir. 1998).

146. Berkey Photo, Inc. v. Eastman Kodak Co., 603 F.2d 263, 287 (2d Cir. 1979).

147. Allied Orthopedic Appliances, Inc. v. Tyco Health Care Grp., 592 F.3d 991, 994–95 (9th Cir. 2010).

148. For a representative argument in favor of using evidence of subjective intent in monopolization cases in the intellectual property context, see W. Michael Schuster, Comment, *Subjective Intent in the Determination of Antitrust Violations by Patent Holders*, 49 S. TEX. L. REV. 507, 530–34 (2007); see also Lao, *supra* note 124.

predatory intent ought not to bear on the antitrust treatment of predatory invention.[149] Taking a view contrary to EU competition rules,[150] and some U.S. decisions,[151] we believe that formal economic analysis alone should provide the pertinent rule of decision in this area. A desire to quash one's rivals is endemic, and proper, in competitive markets.[152]

Economists widely assume that companies act to maximize profit[153]—a subjective aim that entirely subsumes intent to eliminate one's competitors. Such intent is equally consistent with merit-based and exclusionary acts of competition and therefore provides no help in distinguishing the two. Indeed, judicial reliance on corporate "intention" is likely to be especially unreliable, as it may be tempting to regard expressions of nefarious intent as the evidentiary equivalents of outcomes predicted by rigorous economic analysis. Whether a particular innovation is laudable or predatory turns on an economic examination into whether the challenged conduct is welfare enhancing. Since evidence of a company's desire to see its rivals fail is not pertinent to this calculus, it ought to be irrelevant to the analysis of a monopolization case founded on an alleged act of predatory innovation. Judge Easterbrook's pointed exposition of the limits of "intent"-based analysis in monopolization cases is particularly appropriate here:

> [I]ntent plays no useful role in this kind of litigation. Firms "intend" to do all the business they can, to crush their rivals if they can. "[I]ntent to harm" without more offers too vague a standard in a world where executives may think no further than "Let's get more business." Rivalry is harsh, and consumers gain the most when firms slash costs to the bone and pare price down to cost, all in pursuit of more business. Few firms cut price unaware of what they are doing; price reductions are carried out in pursuit of sales, at others' expense. Entrepreneurs who work hardest to cut their

149. *Accord* PHILLIP E. AREEDA & HERBERT HOVENKAMP, ANTITRUST LAW ¶ 775c, at 233 (1996) ("Because courts and juries are generally incapable of addressing the technical merits or anticompetitive effects of innovation, they quickly make the relevant question turn on intent. We believe this is the worst way to handle claims that innovation violates the antitrust laws."). *But see* Ronald A. Cass & Keith N. Hylton, *Antitrust Intent*, 74 S. CAL. L. REV. 657 (2001) (defending a limited role for intent in antitrust cases).

150. *See, e.g.*, Pierre V.F. Bos, *International Scrutiny of Payment Card Systems*, 73 ANTITRUST L.J. 739, 767 n.113 (2006).

151. *See, e.g.*, Image Technical Servs., Inc. v. Eastman Kodak Co., 125 F.3d 1195, 1208–09 (9th Cir. 1997); *see also* Cal. Dental Ass'n v. Fed. Trade Comm'n, 224 F.3d 942, 948 (9th Cir. 2000).

152. *See* Illinois *ex rel.* Burris v. Panhandle E. Pipe Line Co., 935 F.2d 1469, 1481–82 (7th Cir. 1991).

153. *See, e.g.*, Herbert Hovenkamp, *Positivism in Law & Economics*, 78 CALIF. L. REV. 815, 830–31 (1990).

> prices will do the most damage to their rivals, and they will see good in it. You cannot be a sensible business executive without understanding the link among prices, your firm's success, and other firms' distress. If courts use the vigorous, nasty pursuit of sales as evidence of a forbidden "intent," they run the risk of penalizing the motive forces of competition.[154]

If evidence of a company's desire to injure its rivals is as illuminative of consumer-benefitting competition as it is of nefarious exclusion, then courts should eschew such evidence in favor of price-theoretic analysis that seeks to establish the actual market impact of a challenged practice.

C. COERCION

If intent is irrelevant, and the fact that the PTO issued a patent casts little light on the quality of a challenged invention, what other factors should inform antitrust analysis? Might the presence or absence of coercion play an integral role in determining the legality of a challenged innovation? As the cases explored above demonstrate, this factor has formed a focal point of analysis for judicial review of predatory product introductions.

The concept of coercion has intuitive appeal.[155] Few question the difficulty of formulating a reliable judicial method for detecting, let alone quantifying, technological superiority. However, in a market-based economy and a society that puts great weight on individual autonomy, there is at least some consensus that the law should defer to consumers' purchasing decisions, which signal their collective preference for a purportedly improved product.[156] Yet, faith in the market's ability to distinguish high- from low-quality products evaporates when consumers' freedom to choose one product over another is compromised. In cases of perceived coercion, the law ought to be skeptical of claimed improvement. Should deprivation or reduction of consumer choice assume a central place in antitrust analysis of predatory invention?

---

154. *See* A.A. Poultry Farms, Inc. v. Rose Acre Farms, Inc., 881 F.2d 1396, 1401–02 (7th Cir. 1989) (citations omitted).

155. *See generally* Mark R. Patterson, *Coercion, Deception, and Other Demand-Increasing Practices in Antitrust Law*, 66 ANTITRUST L.J. 1 (1997).

156. *See* Barak Y. Orbach, *The Antitrust Consumer Welfare Paradox*, 7 J. COMPETITION L. & ECON. 133, 156 (2011) ("[C]onsumers' revealed preferences . . . may be unwise, they may undermine their own well-being and reduce social welfare, but antitrust laws do not offer relevant preference-shaping mechanisms to address the issue."); *see also* Mark D. Whitener, Editor's Note, *change.gov*, ANTITRUST, Summer 2009, at 4 (quoting Deputy Assistant Attorney General for Economics Carl Shapiro to the effect that antitrust "is not about steering the market in any particular direction other than the direction indicated by consumer preferences").

The answer is no. In the first place, the term "coercion" is unfortunate, since it carries subjective and pejorative connotations, which, like "predatory intent," courts can use to substitute conclusions for analysis. It is, in addition, a term with a broad range of possible meanings, at once ambiguous and opaque. Tying law,[157] for example, uses the term to some disadvantage, though in that context it seems to mean that a dominant firm is forcing consumers to buy something that they would rather not purchase at all or that they would prefer to purchase elsewhere,[158] though its meaning in that context is far from crystal clear.

The term is even more ambiguous with respect to exclusionary product design. In this area, no workable definition of coercion has emerged. Does a company necessarily "coerce" its customers into purchasing the new version of an established product if it withdraws the prior variant of that good? Some might say so, though we think the answer is no. If it were otherwise, the law would place a major impediment on dominant companies' commercialization of improved products. It will not necessarily be economically sensible for a dominant firm to maintain parallel product lines. For example, the costs of keeping two different inventories and of training service personnel to maintain separate products might be prohibitive. It makes no sense for the law to require a dominant firm to keep all of its products on offer forever in order to avoid a finding of "coercion."

Could coercion instead arise from the absence of competition? In a certain sense, strained perhaps, consumers in a pure monopoly market are forced to take the monopolist's product or leave it. Is that limited choice "coercive"? Perhaps, though such a definition would strain the concept of consumer autonomy. Buyers always retain the freedom not to purchase a product at all, regardless of whether it is sold under conditions of monopoly or competition, unless perhaps the relevant good is in some respect essential.

Moreover, even if consensus could somehow emerge around a definition of the term, what degree of coercion should suffice to prevent a court from relying conclusively on consumer demand for a challenged product design as evidence of its legitimacy? This question is especially problematic, for the

157. Product tying occurs when a seller conditions the sale of a product or service ("tying product") on the purchase of a second product or service ("tied product"). The law has traditionally taken a dim view of product tying on account of the perceived fact that the practice (1) deprives consumers freedom of choice, (2) enables the purveyor of the tying product to leverage its dominance into the tied market, and (3) creates barriers to entry. *See, e.g.*, Jefferson Parish Hosp. Dist. No. 2 v. Hyde, 466 U.S. 2, 12 (1984), *abrogated by* Ill. Tool Works, Inc., v. Indep. Ink, Inc., 547 U.S. 28 (2006).

158. *See, e.g.*, Cheryl J. From, Comment, *Is There a Perfect Solution? The Court's Problems in Applying Antitrust Laws to Bundled Discounts*, 7 DEPAUL BUS. & COM. L.J. 145, 153–54 (2008).

concept of coercion does not lend itself to an effective limiting principle, nor are degrees of coercion self-evident. Market imperfections are ubiquitous.[159] Even in competitive industries, companies' relative market shares, marketing strategies, brand names, first-mover advantage, scale and scope efficiencies, and sheer luck can affect consumer demand for a product, and thus compromise the signaling value of the market as a neutral arbiter of quality. Systemic advantages and disadvantages alike complicate the significance of relative consumer demand. Some take the position that many limitations on consumer freedom are compatible with an absence of coercion, and we agree.[160] But impediments beyond the preceding examples can arise, which introduce an unwelcome degree of subjectivity in determining whether consumer choice has been sufficiently compromised.

For instance, companies enjoying collective, or individual, control over innovation platforms may be able to influence the path of third-party product development, in some instances creating a bottleneck that permits them to dictate the nature and qualities of goods filtering down to consumers. Illustratively, some have criticized what they perceive to be inadequate competition between carriers in the wireless industry (AT&T, Verizon, Sprint, and T-Mobile), which allegedly enables those companies to exercise significant control over product design in the wireless equipment and applications markets.[161] Should the fact of high consumer demand for existing products and services satisfy policymakers that excluded devices and applications are of no concern to the antitrust laws? Because such questions are divisive, academics, judges, and enforcers are unlikely to reach common accord on the definition of "coercion" as an element of predatory-innovation analysis.

In sum, when addressing claims of anticompetitive innovation, courts should refrain from relying on the concepts of intent or coercion. Furthermore, courts should decline to infer the existence of an improvement from the fact that a patent covers the relevant product. Finally, although it is well established that a patent bestows a right to exclude, there is no reason in principle why this fact should in itself shield a patentee from any antitrust liability. If a product redesign entails no material benefit over a prior version and carries anticompetitive effect, the presence of a patent over the redesigned product should not foreclose the possibility of an antitrust violation.

---

159. *See* RICHARD A. POSNER, OVERCOMING LAW 428 (1996).

160. *See, e.g.*, Burns v. Cover Studios, Inc., 818 F. Supp. 888, 893 (W.D. Pa. 1993) ("The psychojurisprudence of coercion has no relevance in the field of antitrust law.").

161. *See, e.g.*, Tim Wu, *Wireless Carterfone*, 1 INT'L J. COMM. 389 (2007); *see also* Amol Sharma, *Telecoms Face Antitrust Threat*, WALL ST. J. (July 7, 2009), http://online.wsj.com/article/SB124689740762401297.html.

IV. THE CONTOURS OF AN EFFECTIVE SOLUTION

This Article has explained thus far that each test espoused by the U.S. courts of appeals is unsatisfactory and that optimal antitrust analysis of innovation would decline to consider both coercion and evidence of predatory intent. It would also refuse to draw an inference of technological merit based on patent protection alone. This Part outlines the contours of a better approach.

A. CHARACTERISTICS OF A SUPERIOR ANTITRUST STANDARD

To successfully resolve the problems implicated by antitrust oversight of innovation, one must adhere to a number of foundational principles. First, because overriding social benefits accompany the commercialization of invention,[162] the law should endeavor to promote new products. In this respect, antitrust oversight is an important element in a larger innovation policy.

Second, it is possible for companies strategically to manipulate market processes through purported acts of invention and thus wrongfully to exclude equally or more-efficient competitors. For that reason, an effective competition policy may facilitate greater levels of long-run consumer welfare by fostering an environment conducive to merit-based competition and innovation, and by constraining illusory acts of invention likely to have exclusionary effects. Conversely, an improperly applied antitrust policy may be extraordinarily harmful if it depresses the rate of innovative activity in the economy.

Third, if the judicial process were error-free and if absolute legal certainty prevailed, the optimal antitrust standard would be unequivocal, taking the form of a simple utilitarian calculus that weighed the social benefits of a particular invention against the relevant exclusionary effects. In a hypothetical world in which courts never erred and companies could conclusively determine ex ante the legality of their new technologies or designs, this legal standard would maximize social welfare. Such a standard would lead companies to market only those technological improvements that enhance long-term consumer welfare.

Fourth, in reality, a gap exists between ex post judicial interpretation of facts and their future consequences, on the one hand, and ex ante prediction

162. *See* FED. TRADE COMM'N, THE EVOLVING IP MARKETPLACE: ALIGNING PATENT NOTICE AND REMEDIES WITH COMPETITION 31–48 (2011), *available at* http://www.ftc.gov/os/2011/03/110307patentreport.pdf (explaining the importance of technology transfer and commercialization of the same).

by firms and regulators of how events will play out and how the judiciary will later construe them, on the other. This gap limits innovators' abilities to determine the legality of their current and future actions. Although an absence of legal certainty is a hallmark of legal standards—as opposed to rules—this does not mean that standards are inappropriate. They are pervasive throughout the law and are often desirable, on account of legislatures' limited capacity to envision the full range of future circumstances to which the law will apply and courts' superior ability to mold the optimal parameters of law ex post, when the pertinent facts are clear. In the context of spurring original and follow-on innovation, however, a heightened level of legal certainty would seem very desirable. As a result, society should construct an infrastructure, legal and otherwise, that is conducive to research and development. Judicial second-guessing of the relative merits and costs of a challenged course of innovation would do much violence to this goal.

Fifth, the judiciary's propensity to err in construing and comparing the present and future effects of facts should affect the nature of the optimal antitrust rule or standard. Decision theory[163] informs analysis under conditions of uncertainty and requires policymakers to compare the relative costs and benefits of Type I and II errors. Those categories, for present purposes, refer to the law's erroneously condemning a socially desirable invention and mistakenly permitting a welfare-reducing act of supposed innovation, respectively. Having identified the social harms of erring in these directions, one must then determine the propensity for market self-correction. In this regard, false positives and false negatives may not prove to be equally enduring, which then requires consideration of the net social cost of systematically erring in one direction over the other.[164]

Sixth, the expense of anti-monopolization litigation, the length of time between the onset of allegedly exclusionary behavior and the successful resolution of an ensuing lawsuit, the speed and magnitude of technological change, and the limited remedial powers available to courts to arrest anticompetitive effects are relevant to constructing the optimal legal standard. These factors suggest that, in order for an enforcement action against predatory innovation to be socially desirable, it should seek to halt an anticompetitive practice that possesses exclusionary effects that are apt to have enduring repercussions on competition.

---

163. Decision theory addresses utility maximization under conditions of uncertainty. *See, e.g.*, Adam M. Samaha, *On Law's Tiebreakers*, 77 U. CHI. L. REV. 1661, 1663 n.9 (2010).

164. For the authors' more in-depth discussion of this issue, see Alan Devlin & Michael Jacobs, *Antitrust Error*, 52 WM. & MARY L. REV. 75 (2010).

Collectively, these six principles inform the construction of a responsible antitrust standard. The first two suggest that antitrust laws, properly crafted and applied, could enhance social welfare by spurring greater levels of competition and innovation. The third provides that a simple cost-benefit analysis is most desirable in the absence of judicial error and in the presence of legal certainty.[165] An interesting corollary of this pure cost-benefit standard for legality is that it would allow courts to condemn a valuable act of invention that marks a significant contribution over the prior art, if the invention is apt to yield a period of entrenched monopoly in which dynamic rates of innovation are unlikely to flourish. The D.C. Circuit's current standard governing exclusionary product design reflects this approach.[166]

B. THE SOCIAL-WELFARE CALCULUS UNDER AN ANTITRUST STANDARD

Before discussing how considerations of error, uncertainty, and the practical limitations of litigation complicate analysis and alter the characteristics of the optimal antitrust test, it is illuminative to consider how a legality condition tied to a social-welfare calculus would operate. Specifically, what constitute the relevant costs and benefits that courts would consider in determining whether a challenged invention is, on the whole, welfare enhancing or welfare reducing?

There are two forms of potential benefit—one obvious, the other less so. The first and more obvious form represents, in part, the utilitarian gain realized by the consumption of new technology and improved products. In the modern information economy, advances in commercialized science are apt to be significantly greater contributors to consumer welfare than price differentials.[167] Nevertheless, the social gains of an innovation invariably exceed those realized by the consumers and purveyors of a newly marketed technology because the underlying technical know-how enhances the public storehouse of scientific knowledge, thus informing follow-on research and development.[168] Calculating the aggregate future value of an invention, discounted to present value, poses an intractable challenge, not least because

165. Of course, and as we explore below, pure legal certainty never exists under Section Two of the Sherman Act (15 U.S.C. § 2).

166. *See* United States v. Microsoft Corp., 253 F.3d 34, 58 (D.C. Cir. 2001).

167. *See, e.g.*, Joseph F. Brodley, *The Economic Goals of Antitrust: Efficiency, Consumer Welfare, and Technological Progress*, 62 N.Y.U. L. REV. 1020, 1026 (1987); Joel I. Klein, Assistant Attorney Gen., U.S. Dep't of Justice, Address Before the American Intellectual Property Law Assoc., Cross-Licensing and Antitrust Law (May 2, 1997), *available at* http://www.justice.gov/atr/public/speeches/1118.pdf.

168. *See* Brett Fischman & Mark A. Lemley, *Spillovers*, 107 COLUM. L. REV. 257 (2007).

it is often difficult to predict the future significance of a particular contribution to the relevant art.

The second variant is subtler. It straddles the blurry line between incentive-yielding gains and welfare-reducing monopoly. An important source of potential gain from a challenged product design or other innovation emanates from the economic function of exclusion. This may appear paradoxical, as exclusivity seems axiomatically undesirable, but some closed systems operate as important appropriation mechanisms.[169] By engineering, marketing, or otherwise arranging their products in a particular way, dominant incumbents may be able to delay entry, hinder such entry's effectiveness, or cause it to occur on a reduced scale.[170] In this manner, dominant incumbents can extract a greater proportion of the social value of their products or services and enhance their profits. This may seem always and everywhere to be improper. Indeed, by elevating prices in the short term, exclusion of this sort imposes an undeniable cost in terms of static efficiency. Yet, appropriation mechanisms, which include intellectual property, first-mover advantage, and trade secrets, as well as strategic conduct aimed at extending periods of exclusivity, may be indispensable to innovation.

The problem, from a policy standpoint, arises once again from an intractable uncertainty. In particular, it is not perfectly clear how much of an invention's value an inventor must appropriate in order to have sufficient incentive to invest, nor how much appropriation is "socially correct." It is clear, however, that without some degree of appropriability, incentives to invent and to market inventions will diminish, perhaps to socially harmful levels. To say that an inventor frustrates entry through innovation, then, is not necessarily to condemn the exclusionary act. In at least some situations, innovation that excludes competitors will enhance dynamic, long-run efficiency by promoting incentives to invent and commercialize technologies. Demarcating the limited circumstances in which exclusion is likely to be socially beneficial is a necessary element of analysis.[171]

Against these potential contributions to social welfare, a court wishing to apply a comprehensive balancing test must weigh the costs of a challenged design or invention. The nature of the relevant costs is complicated by the

169. *See, e.g.*, Alexander E. Silverman, Note, *Myth, Empiricism, and America's Competitive Edge: Intellectual Property Antitrust Protection Act*, 43 STAN. L. REV. 1417, 1437 (1991).

170. *See, e.g.*, Thomas J. Campbell, *Predation and Competition in Antitrust: The Case of Nonfungible Goods*, 87 COLUM. L. REV. 1625, 1657 (1987).

171. For a sophisticated discussion of the nature of open and closed systems, see Jonathan M. Barnett, *The Host's Dilemma: Strategic Forfeiture in Platform Markets for Informational Goods*, 124 HARV. L. REV. 1861 (2011).

off-setting and incommensurable significance of short- and long-term negative consequences. The immediate, or static, results of an invention that delays or hinders the availability of substitute products consist of the higher prices that consumers must pay and the forgone utility premium that they would have enjoyed by consuming preferred products that would otherwise have been available. These effects are at least roughly measurable—at least in most settings—but the longer-term consequences of invention-induced exclusion are far harder to quantify.

Because it is almost impossible to predict future paths of innovation and competition in technology markets, the ultimate effect of an exclusionary act is elusive. The requisite analysis concerns not only the path of development and competition for the technology incorporated in the "improved" product, but also that for distinct, follow-on inventions. A representative issue in the *Microsoft* case concerned the effect of the software giant's exclusionary tying practice on "nascent" competition from web-based programs running on Java that could potentially bypass users' operating systems.[172] It was impossible to determine whether such competition would be viable, and whether Microsoft's acquisition of a monopoly over Internet-browsing software would have foreclosed any competition. However, those determinations were crucial to the question whether the challenged action of product design (tying Internet Explorer to Windows) was welfare enhancing and hence lawful, or welfare reducing and thus violative of antitrust laws. The question of long-run effects is indispensable to analysis, but reliable, evidence-based answers are unavailable. Therefore, courts and antitrust enforcers must resort to answers to theoretical, and highly contestable, claims about the relative virtues of concentrated versus competitive market structures, as well as to political predispositions concerning acceptable levels of appropriation through closed systems vis-à-vis open alternatives.

It follows that even a purportedly "simple" test that would weigh the costs and benefits of an invention, and find it lawful if the result of the calculus was positive, is confoundingly difficult to apply. It would require courts to calculate—or rather to estimate—unobservable future consequences and to distinguish harmful exclusion from the kind that permits efficient incentive-generating appropriation. The arduous nature of this task, which far exceeds the realistic fact-finding capacity of courts, implicates the crucial role of error. This Article therefore moves from the unrealistic case of zero error and perfect legal certainty, under which conditions the D.C. Circuit's

172. *See* United States v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001).

approach makes sense, to consider complicating features of actual antitrust practice.

C. A PROPOSED TEST FOR ADDRESSING CLAIMS OF ANTICOMPETITIVE INNOVATION

In light of the preceding discussion, it should be clear that judicial efforts at weighing the costs and benefits of a challenged invention are fraught with danger. Given the precarious nature of the fact-finding involved, economics suggests that courts should heed the lessons of decision theory in fashioning an analytical framework. Broadly, decision theory would require courts to consider the consequences of erring in one direction over another.[173] These consequences are generally circumstance-specific, though as a broad prescription, it is commonly supposed that Type I errors ("false positives") are worse from an antitrust-policy perspective than Type II mistakes ("false negatives").

Applied to the phenomenon of predatory innovation, a Type I error arises when a court condemns a genuine invention, the long-term benefits of which exceed its costs. The magnitude of the error depends on the significance of the invention, as well as on the consequential effects on future innovation—the marginal disincentives—realized by creating a precedent hostile to exclusionary invention. Importantly, the capacity for the market to self-correct is limited to the extent that a certain number of future inventors may decline to invent, as much or at all, in light of the inhibitory ruling.

Conversely, a court commits a Type II error when it allows an illusory invention with exclusionary effects, or a real innovation that carries larger social costs than benefits, to pass muster. Self-correction depends on the exclusionary effect of the erroneously approved product design. If it fetters rivals' abilities to market competing goods, the false negative will likely result in modest harm to competition. Indeed, its second-order effects could be positive by creating a legal environment conducive to invention, thus spurring inventors otherwise worried about legal consequences to market their technologies and to compete aggressively. Of course, against such possible advantages, one would have to weigh the negative incentive generated by an overly permissive rule for dominant firms to devote greater resources to strategic exclusion through meager improvements rather than to focus on genuine acts of welfare-enhancing innovation. Once more, the extent of these repercussions depends on the severity of the relevant error. If a self-described "improvement" was nothing of the kind, and its marketing

173. It also instructs that, when two candidate tests are equally good, or bad, the cheaper ought to be adopted.

carried powerful exclusionary effects, then a Type II error could have significant repercussions.

These features of erroneous decision making lead us to a number of conclusions.

1. A System That Favors False Negatives Is Preferable

First, because the severity of a Type I error rises in proportion with the value of the erroneously condemned invention, a bias in favor of Type II errors is justified when a court finds that an impugned innovation entails a material improvement over the prior art. As a result, a defendant should be able to defeat antitrust liability by establishing that its product design carries significant technical advantages. Even though some such inventions may generate negative consequences that exceed the relevant benefits, those cases are so limited and the nature of a Type I error so much more severe that a systemic preference in favor of false negatives is appropriate.

2. Courts Should Not Distinguish Significant from Trivial Inventions

Second, one might be tempted to qualify this systemic preference for Type II errors by adopting a more stringent antitrust standard to assess what fact-finders determine to be less significant inventions. Scrutinizing such technologies or product designs may warrant less deference to the risk of false positives because the cost of Type I errors would be relatively modest. Policymakers, however, should resist this view. One of the problems with any rule of law that might condemn "small" innovations whose harms arguably outweigh their benefits—setting aside the weighing problems and assuming that a powerful incumbent has made at least a small improvement to its dominant product—is that the dominant company cannot know ex ante whether its innovation, or contemplated innovation, will be deemed significant enough to pass the test (or so small as to fail it). This uncertainty might dissuade it, on the margin, from making "borderline" innovations. Furthermore, in some industries, incremental improvements over the prior art characterize the great majority of innovation, and so even if the cost of a single Type I error in assessing a relatively modest improvement is low, the cumulative effect of many such mistakes could be serious.

3. A Material Improvement Standard Where Invention Eliminates Consumer Choice

Third, Type II errors are apt to be most costly when market mechanisms are ineffective in curing the monopoly conditions created or maintained by an exclusionary product design. The principal justification for preferring Type II over Type I errors lies in the perceived tendency of market forces to erode erroneously permitted anticompetitive practices, as the supranormal

profits facilitated by those practices attract entry and hence competition.[174] If industry conditions are such, however, that entry is unlikely to erode the anticompetitive conditions occasioned by a predatory product design, then the systemic preference in favor of Type I errors may no longer be justified. Illustratively, if a strategic product introduction bolsters a dominant company's position, enabling it to control access to consumers and hence to exclude rivals, courts should not dismiss antitrust suits challenging the innovation as predatory. Applying this principle to legal doctrine, when a challenged innovation prevents an inventor's competitors from marketing their goods to consumers, and thus eliminates consumer choice, a court should scrutinize the invention to determine whether it entails a material—that is, a cognizable—improvement. This follows from the fact that, if a strategic innovation denies consumers access to other companies' products, Type II errors raise heightened concerns, which justifies a court's inquiring into the existence and quality of the claimed innovation. This rule might appear to be similar to the Ninth Circuit's approach in *Tyco*, which deemed a patentable improvement to be inconsistent with an antitrust violation. The material-improvement standard that this Article advocates, however, would only apply when a defendant's action eliminates consumer choice. *Tyco* concerned a situation in which the defendant had not forced consumers to adopt its new product. Under this Article's standard, a strategic product redesign that did not foreclose rivals from selling to consumers would be lawful on that basis alone.

4. Immunity from Antitrust Liability Where Invention Fetters Consumer Choice

Fourth, and conversely, in cases where a product design fetters, but does not eliminate, competitors' ability to offer rival goods to consumers, the new design should be immune from antitrust challenge. This follows from the fact that serious exclusionary effects are most unlikely if the challenged invention does not compromise third parties' ability to market their own products to the consuming public. In that event, competition and consumer choice both remain intact. Moreover, as the costs of Type II errors are apt to be relatively small when competition presents consumers with a choice of

174. Conversely, conventional theory assumes that Type I errors result in permanent inefficiencies because market forces cannot undo an improper legal rule. We have previously questioned the assumption that Type I errors in the antitrust field are impervious to market and other pressures. *See* Devlin & Jacobs, *supra* note 164, at 98–99.

substitute products,[175] a bias against false positives in such circumstances is appropriate. This view follows from the fact that the technological superiority of one company's product necessarily disadvantages its competitors. Public-choice theory predicts that those rivals are likely to seek recourse through the legal system.[176] The history of competition-law enforcement tells a disheartening tale of the judiciary's and enforcement agencies' willingness to entertain such appeals,[177] further justifying per se legality when exclusionary effects are limited.

V. THE UNIQUE CASE OF PRODUCT HOPPING

Having explored the numerous public-policy challenges that antitrust claims of predatory product improvement implicate, and having articulated a proposed standard by which to judge those challenges, this Part considers what many regard as the most blatant instance of anticompetitive innovation: the practice known as "product hopping." This example is simultaneously illuminative and challenging with respect to the Article's proposed standard, for product hopping occurs within the highly regulated pharmaceutical industry. The interplay of antitrust and regulation creates special problems, in particular for the proper treatment of predatory innovation.

Product hopping refers to a drug company's reformulation of its (dominant and patented) product in such a way and at such a time as to simultaneously extend the patent life of that product and to squelch competition from actual and would-be generic rivals. Product hopping can take one or more of several forms: first, the manufacturer may reformulate its drug, changing it from a capsule to a tablet, or to an extended-release or chewable form; second, it can change the molecular make-up of the drug, by adding or removing chemical compounds; and, third, it can combine in one formulation two or more drug compositions that it had previously marketed separately.[178]

Product hopping is but a particular instance of exclusionary innovation. As with the cases of alleged predatory invention explored above, it raises the

175. This is because competition will undo anticompetitive effects brought about by a predatory innovation when that innovation does not foreclose rivals from accessing consumers.

176. *See, e.g.*, THE CAUSES AND CONSEQUENCES OF ANTITRUST: THE PUBLIC CHOICE PERSPECTIVE 180–81 (Fred S. McChesney & William F. Shugart II eds., 1995).

177. *See, e.g.*, WILLIAM H. PAGE & JOHN E. LOPATKA, THE MICROSOFT CASE: ANTITRUST, HIGH TECHNOLOGY, AND CONSUMER WELFARE 28 (2007).

178. *See, e.g.*, Rebecca S. Yoshitani & Ellen S. Cooper, *Pharmaceutical Reformulation: The Growth of Life Cycle Management*, 7 HOUS. J. HEALTH L. & POL'Y 379, 388–403 (2007).

problems of measuring the fact and the quality of invention, and of determining when "small" innovations are "predatory." And, as with those cases, three potential sources of fact-finding exist: courts, the PTO, and consumers.

Product hopping can discourage and defeat generic entry in part because of the requirement that generic entrants comply with state drug-product-selection laws. Those laws, intended to provide consumers with lower-priced drugs, permit and often require pharmacists to substitute generic versions of brand-name prescriptions issued by doctors. In order for this substitution to occur, the generic version of the branded drug must be "AB-rated" by the FDA, which signifies (and requires) that the generic is the therapeutic equivalent of the brand, with the same active ingredient, form, dosage, strength, safety, and efficacy profile. Product hopping—through, for example, a change in the form or the dosage of the branded drug, made just before planned generic entry—can destroy this equivalence or postpone its attainment for a significant period of time. Although pharmacies can sell the generic drug during that time to consumers who specifically request it, they cannot on their own initiative substitute the generic for the brand-name drug, a prohibition that can critically undermine the profitability, or the entry strategy, of the generic.

A. *ABBOTT LABORATORIES V. TEVA PHARMACEUTICALS*: THE DEFINITIVE EXAMPLE OF PRODUCT HOPPING TO EXCLUDE GENERIC COMPETITION

Abbott Laboratories v. Teva Pharmaceuticals USA, Inc.[179] is the poster child for the campaign to condemn product hopping. In that case, the FDA had approved Abbott's capsule version of TriCor—a drug used to lower cholesterol and triglyceride levels—in 1998. Shortly thereafter, two generic firms filed Abbreviated New Drug Applications ("ANDAs"),[180] which challenged the patent underlying the TriCor formulation.[181] In 2003, the courts hearing the claims upheld their challenges, enabling them to market their products.[182] This favorable judicial outcome did not, however, result in the generic entry that might otherwise have occurred. While the litigation was

179. 432 F. Supp. 2d 408 (D. Del. 2006).

180. Companies filing ANDAs certify that a proposed generic drug is bioequivalent to an approved drug, thus allowing a generic-drug manufacturer to take advantage of the pioneer-drug producer's hard-earned safety and efficacy data. *See, e.g.*, Timothy A. Cook, Note, *Pharmaceutical Patent Litigation Strategies: Balancing Patent & Antitrust Policy Through Institutional Choice*, 17 MICH. TELECOMM. & TECH. L. REV. 417, 426 (2011).

181. *Abbott Labs.*, 432 F. Supp. 2d at 415.

182. *Id.* at 416.

pending, Abbott lowered the drug's strength, switched its formulation from capsule to tablet, stopped selling capsules, and repurchased from the pharmacies the entire outstanding stock of capsules.[183] These steps prevented generic substitution, since the generic capsules differed in form and dosage from the brand's new tablets, and since there were no longer any capsules to which the generics' offerings were equivalent.

Discouraged but undeterred, the generics proceeded to develop equivalents to the tablet formulation and submitted new ANDAs to the FDA challenging the patent underlying that formulation.[184] However, while the challenge was pending, Abbott again switched to a new tablet formulation, with a slightly lower dosage of the active ingredient, stopped selling the "old" tablets, and took other steps to foreclose the generics from availing themselves of the state substitution laws.[185] This conduct prompted the generics to sue Abbott for having engaged in a course of "predatory" innovation, a claim which Abbott moved to dismiss on the grounds, among others, that "any product change that introduces an improvement, however minor, is per se legal under the antitrust laws."[186]

After first acknowledging that a serious factual question existed as to whether Abbott's change effected any improvement to its product, the district court assumed for purposes of analysis that there was such an improvement and then applied the *Berkey* test as the basis for analyzing Abbott's motion. The court read *Berkey* to rest on three considerations. First, courts should be reluctant to weigh the anticompetitive harms caused by the introduction of a new product against its technological benefits, where the "weighing had already occurred in the marketplace."[187] Second, this reluctance should depend crucially upon the presence of consumer choice in the relevant market, and the absence of "coercion."[188] Third, greater scrutiny is appropriate "when the introduction of a new product by a monopolist prevents consumer choice."[189]

This analysis implicitly rejects the per se approach Abbott advocated and adopts instead a rule-of-reason methodology that looks to (1) whether the defendant is dominant in a properly defined antitrust market; (2) whether it has introduced a product that in some way "improves" on its predecessor; (3)

183. *See id.* at 415–16.
184. *Id.* at 416.
185. *Id.* at 416–17.
186. *Id.* at 420.
187. *Id.* at 420–21.
188. *Id.*
189. *Id.*

whether that product introduction caused anticompetitive harm to consumers and rival firms; and (4) whether the harm was attributable to an absence of consumer choice caused by the dominant firm. Because Abbott's conduct as described above—buying back the older formulations in order to prevent generic substitution—might plausibly have eliminated or reduced consumer choice, the court denied Abbott's motion to dismiss.[190]

B. ACADEMIC HOSTILITY TOWARD PRODUCT HOPPING

The academy has been critical of product hopping and has generally urged courts to apply antitrust laws so as to forbid it.[191] Noteworthy in this respect is Professor Michael Carrier's recent article, which contends that product hopping has added a new and unsettling dimension to the problem of "reverse payments," a development which over the past five years has generated significant commentary, litigation, appellate opinions, inter-agency disputes, and failed legislation, but no consensus around a proposed solution.[192] Simply put, a reverse payment occurs when a brand-name (pioneer) pharmaceutical firm and a generic company settle patent infringement litigation by agreeing that the pioneer will pay the generic a (usually) sizeable sum to drop its patent challenge and to delay entering the market for some period of years.[193]

In Carrier's view, while reverse payments and product hopping are each apt to be anticompetitive on their own, they are even more anticompetitive in combination.[194] Thus, he argues, a reverse-payment settlement that prevents patent challenges for a period of time—even if it allows generic entry before the expiration of the patent—"gives the brand firm the space in which it can comfortably switch the market to the new product" by the time such entry

190. *Id.* at 434.

191. *See, e.g.*, Stacey L. Dogan & Mark A. Lemley, *Antitrust Law and Regulatory Gaming*, 87 TEX. L. REV. 685, 687–88 (2009); Steve D. Shadowen, Keith B. Leffler, & Joseph T. Lukens, *Anticompetitive Product Changes in the Pharmaceutical Industry*, 41 RUTGERS L.J. 1 (2009); Michael Stumo, *Anticompetitive Tactics in Ag Biotech Could Stifle Entrance of Generic Traits*, 15 DRAKE J. AGRIC. L. 137, 147–48 (2010); *cf.* Jessie Cheng, *An Antitrust Analysis of Product Hopping in the Pharmaceutical Industry*, 108 COLUM. L. REV. 1471 (2008). *But see* Daniel A. Crane, *Provigil: A Commentary*, 3 HASTINGS SCI. & TECH. L.J. 453, 454–57 (2011) (arguing that the courts should not "get into the business of scrutinizing 'product hopping' ").

192. *See* Michael A. Carrier, *A Real-World Analysis of Pharmaceutical Settlements: The Missing Dimension of Product Hopping*, 62 FLA. L. REV. 1009 (2010).

193. *See In re* Ciprofloxacin Hydrochloride Antitrust Litig., 604 F.3d 98 (2d Cir. 2010), *cert. denied*, 131 S. Ct. 1606 (2011); Ark. Carpenters Health & Welfare Fund v. Bayer AG, 544 F.3d 1323 (Fed. Cir. 2008); Schering-Plough Corp. v. Fed. Trade Comm'n, 402 F.3d 1056 (11th Cir. 2005); *In re* Cardizem CD Antitrust Litig., 332 F.3d 896 (6th Cir. 2003).

194. *See generally* Carrier, *supra* note 192.

can occur.[195] As a consequence, the generic's entry will become difficult, unprofitable, or both, and therefore less likely. In this way, Carrier claims, the combination of reverse payments and product hopping creates "a significant roadblock to pharmaceutical competition."[196]

As evidence of the anticompetitive nature of these practices, Carrier offers two case studies involving the interplay between reverse payment settlements and product hopping.[197] In each, the pioneer manufacturer, faced with imminent competition from generics and the consequent loss of millions of dollars of monopoly rents, sued the generics for infringement. The pioneer manufacturers then made large reverse payments to settle the cases on terms that allowed generic entry years before the expiration of the payment but that also preserved the pioneer's exclusivity for a period of years. They then used that period—along with pricing and promotion strategies—to switch the market to a newly patented formulation that offered only "modest improvements" to patients.[198] In each case, generic entry came too late or not at all and was competitively ineffective, failing to afford consumers the lower prices that presumably would have obtained in the absence of the settlement.

One of the linchpins of Carrier's argument is that product hopping is a charade. Pioneer firms deploy it to persuade consumers (and doctors) to ignore their best interests and buy (or prescribe) a high-priced new drug—protected by a weak formulation patent—that is either no better or not sufficiently better than its predecessor to justify the high price and the generic competition sacrificed by the settlement.[199] Carrier thus implicitly casts product hopping as a form of predatory innovation, suggesting that it allows dominant firms to unfairly exclude equally efficient rivals by making unimportant changes to their dominant but at-risk products.

C. ANALYZING PRODUCT HOPPING UNDER THIS ARTICLE'S PROPOSED ANTITRUST STANDARD

Product hopping displays all of the typical hallmarks of predatory innovation and is thus a representative form of strategic exclusion that is worthy of consideration. Most cases of predatory innovation entail allegations that the defendant designed a challenged product to disadvantage its rivals. One finds such accusations in a wide variety of classic cases from

195. *Id.* at 1009.
196. *Id.*
197. *Id.* at 1022–30.
198. *Id.* at 1023–24.
199. *Id.* at 1020–21.

IBM's challenged design of its CPUs in the 1970s to Microsoft's integration of its Windows and Internet Explorer products in the 1990s. Product hopping is no different, as few doubt that a principal motivation for the practice is the desire to exclude competition. Furthermore, resolving antitrust claims founded on product hopping requires, at least in the first instance, a comparison between the qualitative benefits of the relevant reformulation, if any, and the costs imposed by the same in excluding competition. Issues of judicial competence and error costs greatly influence analysis of product hopping, as they do claims of anticompetitive invention more generally. For these reasons, the phenomenon is a fitting candidate for illustrative application of our proposed antitrust standard. The fact that product hopping is today one of the most controversial practices at the intersection of antitrust and intellectual property makes it an ideal object of consideration.

Antitrust analysis of product hopping poses unique difficulties because of the complex regulatory environment within which the practice occurs. These complications are themselves illuminative of the larger problem of regulating the process of innovation through competition laws. U.S. antitrust jurisprudence has developed a series of principles aimed at fostering efficient market processes, in part by ensuring that dominant companies cannot exclude equally or more efficient competitors. These principles, which are simultaneously hostile to free riding and generally receptive of companies' efforts to appropriate the value created by their investments, may find themselves in conflict when applied to regulated industries.

In our view, regulatory gaming, of which strategic drug reformulation is a particularized example,[200] is a phenomenon that competition law is ill-suited to address.[201] By encouraging generic drug makers to challenge patents held by brand manufacturers, the legal infrastructure governing the pharmaceutical industry—the Hatch-Waxman Act in particular[202]—goes to great lengths to foster free riding on what may be a uniquely large scale. Indeed, companies operating in the pharmaceutical industry are subject to no less than three distinct forms of regulation—the FDA, state generic-substitution laws, and the PTO—which are collectively designed to foster a qualified form of piggybacking on others' investments. As explained below, antitrust law cannot condemn certain forms of product hopping without

200. *See generally* Dogan & Lemley, *supra* note 191.

201. For an interesting discussion of how the law ought to deal with regulatory gaming, see Donald T. Hornstein, *Resiliency, Adaptation, and the Upsides of Ex Post Lawmaking*, 89 N.C. L. REV. 1549, 1575–76 (2011).

202. Drug Price Competition and Patent Term Restoration (Hatch-Waxman) Act, Pub. L. No. 98-417, 98 Stat. 1585 (1984) (codified as amended at 35 U.S.C. § 156 (2010)).

radically altering long-existing tenets of its jurisprudence. We suggest that rewriting the law in this way is undesirable, and so the practice of product hopping requires a regulatory, rather than an antitrust, solution.

Before explaining this result, one must address the potential value of the formulation patents generally associated with product hopping, for if those patents necessarily lack merit, one could safely condemn a large fraction of all product hopping. According to the medical literature, however, changes in drugs from one form of delivery to another can yield real, albeit modest, benefits to doctors and their patients.[203] It is not the case, therefore, that product hopping necessarily amounts to a redesign utterly lacking in qualitative benefit. As a consequence, courts engaged in antitrust analysis of this phenomenon must concern themselves with Type I errors, which would occur if they condemned a company for marketing a newly formulated drug that provides consumers with new and genuine benefits. The judiciary must also be conscious of the risks posed by a vague antitrust rule potentially hostile to drug reformulations, as such precedent could dissuade pharmaceutical companies from withdrawing prior drugs from the market and replacing them with what they consider to be better versions based on delivery method, dosage, or other relevant criteria.[204] Indeed, it may be difficult for pioneer-drug manufacturers to determine whether or not a planned replacement of one version of a drug with another will invite cries of illegal product hopping from generic-drug producers who are planning to enter the relevant market.[205]

With these issues in mind, we apply our proposed antitrust standard for overseeing allegedly anticompetitive product designs to the product-hopping phenomenon. The first aspect of this approach asks whether a dominant company's introduction of a new product eliminates competitors' abilities to offer their goods to consumers. This inquiry is relatively straightforward in unregulated markets but rather more difficult in the pharmaceutical setting. As noted above, the FDA controls entry into drug markets and will allow ANDA filers to market a particular generic drug only if there is a

203. *See, e.g.*, Gina Shaw, *Drug Reformulation: It's Not Just About Patent Protection*, DRUG DISCOVERY & DEV. (Jan. 1, 2007), http://www.dddmag.com/drug-reformulation-its-not-just.aspx.

204. *See, e.g.*, Guy V. Amoresano, *Branded Drug Reformulation: The Next Brand vs. Generic Battleground*, 62 FOOD & DRUG L.J. 249, 256 (2007).

205. *See* Crane, *supra* note 191, at 454–57.

bioequivalent[206] and pharmaceutically equivalent[207] pioneer drug listed in the Orange Book.[208] By hopping, a brand-name-drug manufacturer can remove the pioneer drug listed in the Orange Book and replace it with a reformulated version. If the hop occurs after the FDA has approved the ANDA application, the "generic" manufacturer can still enter the market and sell its equivalent of the now-withdrawn drug. In such a case, the ANDA filer's marketed drug and the reformulated brand-name drug will typically occupy the same antitrust market because the latter drug's new features are unlikely to differentiate it sufficiently to render it non-substitutable.

So, does product hopping foreclose consumer choice? The answer might depend on the timing and effect of the hop. If the incumbent monopolist were to hop after an aspiring generic drug manufacturer filed an ANDA, but before the FDA granted authorization, the brand-name-drug producer would successfully exclude the ANDA filer from the market. In such a situation, the generic-drug company must either file a New Drug Application ("NDA"), thus subjecting it to a cost similar in terms of time and treasure to that experienced by the pioneer-drug manufacturer, or file an ANDA over the new drug. In either event, because the generic-drug company cannot market the particular drug that it wished to sell, the product hop denies consumers a choice of otherwise competitive drugs.

For hops of this nature, our test would require a court to scrutinize the reformulated drug to determine if the changes comprised within it provide a material—that is, a discernible or cognizable—benefit to consumers. For reasons explained above, the fact that the drug manufacturer obtained a patent over the new version is not controlling as to this question. The court would have to entertain expert testimony from medical professionals and pharmacologists as to the nature of the relevant formulation and whether it met a previously unaddressed consumer need (i.e., preference for chewable pills over capsules) or otherwise benefitted patients in a material manner. If

206. Two drugs are bioequivalent (pharmaceutically equivalent) if they contain the same active ingredient and have the same dosage form, strength, and route of administration. 21 C.F.R. § 320.1 (2011).

207. Two drugs are therapeutically equivalent if they are pharmaceutical equivalents and have the same clinical effect and safety profile in administration. *Drugs: Glossary of Terms*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/Drugs/informationondrugs/ucm079436.htm (last updated Feb. 2, 2012).

208. *See, e.g.*, David M. Dudzinski, *Reflections on Historical, Scientific, and Legal Issues Relevant to Designing Approval Pathways for Generic Versions of Recombinant Protein-Based Therapeutics and Monoclonal Antibodies*, 60 FOOD & DRUG L.J. 143, 194–95 (2005). The official name for the Orange Book is *Approved Drug Products with Therapeutic Equivalence Evaluations*, and it is available online at http://www.accessdata.fda.gov/scripts/cder/ob/default.cfm (last updated Feb. 2012).

the fact-finder were to determine that the new product offered illusory benefits and was simply a pure substitute over the replaced version, an antitrust violation should follow.

There is another form of hop, however, that would automatically pass scrutiny under the proposed standard—an aspect of our approach that may be controversial in some quarters.[209] This version of product hopping would occur if the incumbent's reformulation and replacement of its drug occurred after the FDA had approved the generic's ANDA. In this instance, the ANDA filer would be free to market its drug, though the incumbent's withdrawal of the pioneer drug means that the ANDA filer would be unable to sell its product as a generic. The effect of the hop would thus be to deny the entrant access to generic-substitution laws that facilitate rapid acquisition of market share from the incumbent pioneer-drug manufacturer and similarly to prevent the entrant from marketing its product as a generic equivalent of the brand-name drug. Without these advantages, generic-drug companies invariably fail to make significant inroads, and so entering the market under its own brand name is unattractive. Instead, such companies generally either file an ANDA for the reformulated brand-name drug or simply decline to enter the market. Either way, one might fairly argue, consumers lose.

Should this be an antitrust violation? Under our proposed standard, the answer is no. Because this kind of hop cannot exclude an equally or more efficient rival, it fails to arouse the concern at the heart of Section Two jurisprudence.[210] George Stigler famously defined an entry barrier as a practice that causes a prospective or actual entrant to experience costs greater than those that the incumbent incurred.[211] This version of product hopping does not satisfy Stigler's definition because it cannot cause generic-drug companies to incur costs in excess of those expended by pioneer drug manufacturers, which on average amount to several hundreds of millions of dollars per drug. ANDA filers free ride on the massive investment and risk experienced by NDA filers, as well as on the advertising expenditures undertaken by the brands to establish familiarity with their drugs' therapeutic qualities and brand names.[212] A hop that does not foreclose regulatory approval to market a drug requires the entrant to expend considerable

209. *See, e.g.*, Jacobson, Sher & Holman, *supra* note 31, at 27–28.

210. *See* RICHARD A. POSNER, ANTITRUST LAW 194–95 (2d ed. 2001) (defining an objectionable exclusionary practice as one capable of excluding an "equally or more-efficient competitor").

211. George J. Stigler, *A Theory of Oligopoly*, 72 J. POL. ECON. 44, 47 (1964).

212. *See, e.g.*, Samuel Mark Borowski, Comment, *Saving Tomorrow from Today: Preserving Innovation in the Face of Compulsory Licensing*, 36 FLA. ST. U. L. REV. 275, 292 n.134 (2009).

resources on promoting its product as a desirable substitute for the reformulated brand-name drug. The business model on which generic-drug companies operate, of course, does not allow for such expenditures, but this should not change the nature of the antitrust inquiry. The problem, if one exists, is that antitrust rules are designed to operate in unregulated markets in which companies enjoy equality of opportunity.

The key insight here is that policymakers should not distort well-established antitrust rules in order to solve what is, at heart, a regulatory problem. Courts do not manipulate other fields of law to prohibit, for example, strategic tax planning that takes advantage of unintended loopholes in the tax code. One would hardly find someone liable for violating the spirit, but not the letter, of duly enacted legislation. Instead, the proper solution is for the legislature to amend the operative statute to end perceived abuses and manipulation of the legal infrastructure. Product hopping in the pharmaceutical industry is an excellent candidate for such a solution.

VI. CONCLUSION

Innovation is the engine of our economy.[213] Nothing accounts for more growth or improvement in the lives of consumers. Over the past thirty years, antitrust law, which aims to protect consumer welfare, has come explicitly and robustly to recognize and appreciate the crucial role that invention and the intellectual property rights that protect and encourage it play in fostering that welfare. Predatory innovation, however, can hurt consumers. At least in theory, dominant firms can exclude rivals and maintain their dominance by strategically introducing "new" but unimproved products that deprive their smaller rivals of market share, thus discouraging their entry and reducing consumer choice.

Since predatory innovation is harmful, courts should punish it when it occurs. This approach would be simple if the world of innovation were easily divisible into "good" and "bad," "harmful" and "benign." Unfortunately, it is not. Challenged innovations can range from the completely uninventive to the tremendously creative, including everything in between as well as a class whose benefits are yet to be determined.

How are courts to respond then to claims of predatory innovation? If they afford dominant firms too much leeway, consumers may lose the valuable competition that the smaller plaintiff-firms would have provided. Yet if they are too strict, they will force consumers to forgo the value of real

213. *See, e.g.*, DOJ, *supra* note 1; *see also* Hilton Davis Chem. Co. v. Warner-Jenkinson Co., 62 F.3d 1512, 1529–32 (Fed. Cir. 1995) (Newman, J., concurring).

inventions in the short run while creating disincentives in the long run for dominant firms to invest in research and market new products.

These questions are further complicated by the varying and conflicting levels of institutional competence that might plausibly bear on their resolution. Courts are not expert in determining the fact and extent of a new product's inventiveness. The PTO might have more expertise, but the issuance of a patent is not always a sign that the patented product is truly innovative. Consumer preference might be a useful guide, but consumers can be irrational in their product choices, which are themselves determined by the marketing decisions of the firms that sell the products.

Over the past three decades, four separate U.S. courts of appeals have authored tests designed to resolve claims of predatory innovation. Each of those tests differs significantly from the others. None works. The Federal Circuit focuses on predatory intent, an elusive and ambiguous feature unconnected to market outcomes. The Second Circuit looks most closely at coercion, another ambiguous term with a wide range of potential application and therefore almost no transparency. The Ninth Circuit inquires as to whether the "predator's" product offers any smidgeon of improvement. If it does, there can be no predation; but if it does not, the test is silent about what happens next. Finally, the D.C. Circuit, most ambitiously, has adopted a balancing test, which weighs the consumer benefits of the innovation—after the fact of innovation has been determined—against its harms, in a complex calculus. This test is also opaque, and its only saving grace, thus far, is that the court has had no occasion to deploy it.

These tests all fail for the same reason. Each avoids grappling with the four real questions of interest raised by charges of predatory innovation: (1) has the dominant firm offered consumers an improved product?; (2) if so, how much improvement is necessary to immunize it from the charge of predation?; (3) how and by which institution should the fact of improvement be determined—courts, neutral experts, the PTO, consumers?; and (4) if there has been no improvement, what kinds of competitive effects must follow in order for courts to find predation? The recent phenomenon of product hopping, which is an industry-specific form of predatory innovation, raises all these questions and additional ones as well, given the involvement of the FDA in approving the products for use and of the state pharmacy laws in regulating the sale and substitution of generic drugs.

This Article has described the judiciary's failed efforts to formulate a coherent approach to predatory innovation claims, has analyzed the existing case law, and has explored the institutional conflicts and limitations. It has proposed an improved approach, one that defers to true invention and makes claims of predation hinge on its absence. In the process, this Article

has rejected tests that look to "predatory intent" and "consumer coercion" as meaningless, unworkable, or both.

At the center of this Article's test is the issue of exclusion, the issue at the heart of Section Two jurisprudence. If the alleged "predator" has not, through its product introduction no matter its inventiveness, excluded an equally efficient firm from the market, it has committed no wrong. Predatory innovation can arise only when there has been exclusion, and only then when the offending product offers consumers nothing new and valuable. This test is not only much simpler to understand and apply than any of those thus far adopted, but more importantly it focuses on the factors that ought to matter to antitrust law: invention, exclusion, and the limits of institutional competence.

MIXED REALITY: HOW THE LAWS OF VIRTUAL WORLDS GOVERN EVERYDAY LIFE

Joshua A.T. Fairfield[†]

ABSTRACT

Just as the Internet linked human knowledge through the simple mechanism of the hyperlink, now reality itself is being hyperlinked, indexed, and augmented with virtual experiences. Imagine being able to check the background of your next date through your cell phone, or experience a hidden world of trolls and goblins while you are out strolling in the park. This is the exploding technology of Mixed Reality, which augments real places, people, and things with rich virtual experiences.

As virtual and real worlds converge, the law that governs virtual experiences will increasingly come to govern everyday life. The problem is that offline and online law have significantly diverged. Consider the simple act of purchasing something. If you purchase a book offline, you are its owner. If you purchase an e-book, you own nothing. As Mixed Reality technologies merge realspace and cyberspace, the question is whether online or offline law will determine consumers' rights over their property and data. There is a very real risk that courts will continue to reason from online analogies rather than turning to offline common law rules to determine consumers' rights.

This Article offers a modest proposal for rebalancing the law. The common law proceeds by reasoned progression based on the closest available analogy. The Article suggests that the common law has long evolved internal checks and balances for rules that govern citizens' everyday lives. The Article proposes rebalancing the law of Mixed Reality by using analogies to real world situations, rather than limiting legal analysis to intellectual property and online licensing law.

"We have got to stop using the Internet like a typewriter!"
—Anonymous

† Associate Professor of Law and Director, Frances Lewis Law Center, Washington & Lee University School of Law. Thanks to all of the participants at SHARP 2009, *Mixed Reality: When Virtual Plus Real Equals One*, for incredible insight and inspiration. Many thanks to Ted Castronova, Greg Lastowka, Leo A. Holly, and Scott Boone for ongoing conversations and suggestions. Thanks to Kelley Bodell, Michael Bombace, and Vidal Maurrasse for research assistance. All errors, opinions, and errors of opinion are mine.

TABLE OF CONTENTS

I. INTRODUCTION

Imagine a museum. The museum has statuary, pictures, and a fountain located in the atrium. As you enter the museum, you adjust your glasses that offer you four different experiences. You select the first channel. A virtual

docent appears and begins to provide a lecture accompanied by multimedia presentations of each of the exhibits.[1] You can also see wiki-style notes and comments on each note written and rated for usefulness by former museum visitors.[2] Curious, you flip to channel two—intended for children. There, you experience conversations with the artworks themselves, which animate and engage you in entertaining banter. The third channel contains entirely virtual exhibits that occupy physical spaces in and around the museum. The fourth and last channel displays an avant-garde mash-up in which artists from across the city have experimented with and built on the exhibits, altering pictures in subtle ways, adding lighting to statues to change the effect, or outright modifying the exhibits so that they are half real, half virtual.[3] Although this type of technology may sound like science fiction, New York's Museum of Modern Art ("MoMA") has already featured such an installation.[4]

Now, let us interject reality. The scene described above will never be the future. In the future rather than four channels there will be thousands of channels offering experiences in the museum from the fantastical to the statistical, and everything in between. The merging of the Internet with the physical world around us—"realspace"—is called Mixed Reality. Mixed Reality technology is already in use and its adoption is only accelerating.[5]

Imagine a world in which your clothes are free but your clothes carry shifting advertisements on smart fabric. Imagine a world in which your communication and interaction with others are so extensively digital that you can choose to edit your ex-husband out of your existence—you won't have to see him, hear him, see anything he has written, hear any phone calls, nothing. The future of Mixed Reality, where virtual world technologies

1. *See* Alexander Fidel, *Art Gets Unmasked in the Palm of Your Hand*, N.Y. TIMES (Dec. 1, 2010), http://www.nytimes.com/2010/12/02/arts/02iht-rartsmart.html (discussing the use of smartphones, overlaying digital content onto real spaces that effectively connects the content to a realspace anchor, creating "augmented reality"—for example, a museum patron who points his or her smartphone at a sculpture, and the artist appears on the screen ready to be interviewed).

2. *Id.* (discussing the use of Layar, an augmented reality app that can tap into multiple layers of reality tied to realspace locations, like the MoMA).

3. *Id.*

4. *Id.* (identifying the MoMA's application as one of the most popular).

5. *See* Woodrow Barfield, *Commercial Speech, Intellectual Property Rights, and Advertising Using Virtual Images Inserted in TV, Film, and the Real World*, 13 UCLA ENT. L. REV. 153, 158–59 (2006) (discussing the use of a mobile computer that is used in conjunction with a wireless network resulting in the use of information from the Internet to mediate reality, such as virtual advertising on real objects); *see also* 3 JANNA QUITNEY ANDERSON & LEE RAINIE, UBIQUITY, MOBILITY, SECURITY: THE FUTURE OF THE INTERNET 297–99 (2009).

govern our everyday life, is already here.[6] Through mobile technology, computing has finally come out from behind a desk and into the street.[7] As a result, the laws that govern virtual worlds have a greater and greater impact on our everyday lives.[8] However, the law is playing a desperate game of catch-up in order to adapt as disputes and lawsuits over Mixed Reality arise.[9]

Most scholarship to date has assumed that modern society is increasingly virtualized.[10] It is more accurate to note that virtual data is increasingly realized as it becomes tied to realspace features and geography.[11] Yet while virtual experiences are entering real life at an ever-increasing pace, the legal literature on virtualization technologies lags badly. The bulk of virtual worlds research focuses on the impact that real world regulatory regimes have on online spaces and communities.[12] This Article proposes that the traditional

---

6. BRIAN X. CHEN, ALWAYS ON 4–7 (2011) (discussing the far-reaching impact of the iPhone and its role in weaving data with physical reality).

7. Sometimes, *literally* into the street, as in the example of augmented reality windows in upcoming Toyota vehicles. *See Toyota's 'Window to the World' Offers a Taste of Driving Technology to Come*, INDEPENDENT (London) (July 28, 2011), http://www.independent.co.uk/life-style/motoring/toyotas-window-to-the-world-offers-a-taste-of-driving-technology-to-come-2327504.html ("In the future . . . drivers can expect windshields to act in a similar manner, able to overlay digital information for practical, rather than educational or entertainment purposes.").

8. *See* Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593 (E.D. Pa. 2007) (detailing the use of a Term of Service, or "TOS"). TOSs—or End User License Agreements ("EULAs") as they are often called—are the dominant form of legal relationship in virtual worlds. *See* Joshua A.T. Fairfield, *Anti-social Contracts: The Contractual Governance of Virtual Worlds*, 53 MCGILL L.J. 427, 429 (2008) (discussing the prevalence of EULAs in virtual worlds). EULAs, as contracts, define the terms of the relationship between the company and the user. Not unlike Linden Research's game Second Life, mobile phone carriers and the creators of mixed reality applications use EULAs and TOSs to control their software. This is already evident in any app downloaded from the Apple Store. *See Legal Information & Notices*, APPLE.COM, http://www.apple.com/legal/terms/site.html (last updated Nov. 20, 2009).

9. *See, e.g.*, Rosenberg v. Harwood, No. 100916536, 2011 WL 3153314 (D. Utah May 27, 2011) (awarding Google's motion to dismiss because Google was found not negligent). The Plaintiff sued Google after she used the Google Maps direction feature and was struck by a car. *See also* Kirit Radia, *Google Nearly Starts a War. Seriously.*, ABC NEWS: NOTE (Nov. 11, 2010, 12:43 PM), http://blogs.abcnews.com/thenote/2010/11/google-nearly-starts-a-war-seriously.html (describing how two nation-states in Central America almost started a war after Google Earth showed a border in the wrong location).

10. *See, e.g.*, Jack M. Balkin, *Virtual Liberty: Freedom To Design and Freedom To Play in Virtual Worlds*, 90 VA. L. REV. 2043 (2004); Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CALIF. L. REV. 1 (2004); Juliet M. Moringiello, *What Virtual Worlds Can Do for Property Law*, 62 FLA. L. REV. 159 (2010).

11. *See* Doug Gross, *New Wave of Location-Based Apps Mark a 'Paradigm Shift,'* CNN TECH (July 29, 2011, 9:46 AM), http://www.cnn.com/2011/TECH/mobile/07/29/discovery.apps/index.html; *see also* Fidel, *supra* note 1.

12. *See* Lastowka & Hunter, *supra* note 10, at 1, 11, 29 (discussing the permeable nature between virtual worlds and the real world and the role of "real-world" law such as property);

focus is backwards—that the legal regimes governing virtual worlds are increasingly coming to govern real world day-to-day life. This trend is accelerating as Mixed Reality applications integrate virtual objects and experiences into the real world.[13]

The growing application of online law to realspace is a problem because offline and online law have significantly diverged. Consider the simple act of purchasing a book. If you purchase a book offline, you own the book. If you purchase an e-book, you own nothing.[14] As Mixed Reality technologies merge real and cyberspace, the critical question is whether online or offline law will determine consumers' rights over property and data. There is a very real risk that courts will continue to reason from online analogies for offline issues, rather than turning to offline common law rules to determine consumers' rights.

This Article proposes rebalancing the law governing Mixed Reality by using analogies to real world situations rather than limiting legal analysis to intellectual property and online licensing law. Because the common law proceeds by reasoned progression based on the closest available analogy, it seems more in line with the American legal tradition to look to "real world" law for Mixed Reality, despite the increasing virtual enhancement enabled by Mixed Reality applications. For example, imagine that a disgruntled neighbor defaces your home with an obscene word that appears when your house is viewed using a Mixed Reality application. The most appropriate analogy may be to the law of property and trespass rather than referring to the online licensing agreements of the application creator.

In proposing a rebalancing, this Article bridges serious gaps in two sets of legal literature. First, there is a gap in the legal literature with respect to the impact of Mixed Reality applications. Over 200 articles have been published on law and virtual worlds or virtual reality in recent years.[15] To date none

Leandra Lederman, *"Stranger Than Fiction": Taxing Virtual Worlds*, 82 N.Y.U. L. REV. 1620, 1623–24 (2007) (outlining potential frameworks for taxation within virtual worlds).

13. *See* Jason W. Croft, *Antitrust and Communications Policy: There's an App for Just About Anything, Except Google Voice*, 14 SMU SCI. & TECH. L. REV. 1, 1–4 (2010) (discussing the widespread growth in smartphones, in particular the iPhone, and the extensive offerings of the app store); *see also* Dan Fletcher, *10 Tech Trends for 2010*, TIME (Mar. 22, 2010), http://ti.me/AfOUk4 (detailing the rise in augmented reality particularly among iPhone apps).

14. Gregory K. Laughlin, *Digitization and Democracy: The Conflict Between the Amazon Kindle License Agreement and the Role of Libraries in a Free Society*, 40 U. BALT. L. REV. 3, 5 (2010) ("Amazon . . . retains ownership of the 'Digital Content' (i.e., the e-book) and imposes a number of restrictions that are inconsistent with transfer of ownership to the purchaser, including prohibiting redistribution.").

15. *See, e.g.*, Balkin, *supra* note 10; Bryan T. Camp, *The Play's the Thing: A Theory of Taxing Virtual Worlds*, 59 HASTINGS L.J. 1 (2007); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U.

have focused on the legal impact of Mixed Reality applications[16] even though Mixed Reality is far more common and commercially important than are pure virtual worlds.[17] This gap is all the more important because computing has begun a great migration away from desktop computers and towards laptops, tablets, and most of all, smartphones.[18] Mobile computing has led to the augmentation of real people, places, and things with virtual experiences and data.[19] For example, when you compare prices on eBay or Amazon from your desktop, there is not a pressing need to tie the data to a specific location. But if you use a smartphone barcode scanner to compare prices as you shop in the local supermarket, the actual, physical location of competing products at lower prices matters. Stores that augment their brick-and-mortar

CHI. L. REV. 1199 (1998); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993 (1994); Steven Hetcher, *User-Generated Content and the Future of Copyright: Part Two—Agreements Between Users and Mega-sites*, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 829 (2008); Andrew E. Jankowich, *Property and Democracy in Virtual Worlds*, 11 B.U. J. SCI. & TECH. L. 173, (2005); Sarah K. Jezairian, *Lost in the Virtual Mall: Is Traditional Personal Jurisdiction Analysis Applicable to e-Commerce Cases?*, 42 ARIZ. L. REV. 965 (2000); Lastowka & Hunter, *supra* note 10; Juliet M. Moringiello, *What Virtual Worlds Can Do for Property Law*, 62 FLA. L. REV. 159 (2010); Michael H. Passman, *Transactions of Virtual Items in Virtual Worlds*, 18 ALB. L.J. SCI. & TECH. 259 (2008); David G. Post, *Against "Against Cyberanarchy,"* 17 BERKELEY TECH. L.J. 1365 (2002); Steven R. Salbu, *Who Should Govern the Internet?: Monitoring and Supporting a New Frontier*, 11 HARV. J.L. & TECH. 429 (1998); Andrew D. Schwarz & Robert Bullis, *Rivalrous Consumption and the Boundaries of Copyright Law: Intellectual Property Lessons from Online Games*, 10 INTELL. PROP. L. BULL. 13 (2005); Allan R. Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L L. 1167 (1998); Richard S. Zembek, *Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace*, 6 ALB. L.J. SCI. & TECH. 339 (1996).

16. *See* Barfield, *supra* note 5 (discussing the use of augmented reality exclusively in the virtual advertising context).

17. *Compare* GREG LASTOWKA, VIRTUAL JUSTICE: THE NEW LAWS OF ONLINE WORLDS 9 (1st ed. 2010) ("[I]n 2009, by conservative estimates, about 100 million people were interacting in some sort of virtual world . . . [and] about 10 percent of adults in the United States have participated in some kind of virtual world."), *with* Michael K. Cheng, *iPhone Jailbreaking Under the DMCA: Towards a Functionalist Approach in Anti-circumvention*, 25 BERKELEY TECH. L.J. 215 (2010) (discussing the rapid growth to date, predicted growth, and impact of smartphones along with their associated app stores), *and* Elaine Glusac, *Travel Apps 2.0*, N.Y. TIMES: IN TRANSIT (Jan. 4, 2010, 4:17 PM), http://intransit.blogs.nytimes.com/2010/01/04/travel-apps-20/ (discussing how augmented reality is "the hot new thing" for smartphones, and specifically the targeting of augmented reality travel apps to everyday travelers), *and* Jane L. Levere, *Penney Sells Back-to-School Clothes the Digital Way*, N.Y. TIMES (Aug. 2, 2010), http://nyti.ms/y41xjU (detailing the use of augmented reality to sell clothes to teenage girls).

18. *See* Evelyn M. Rusli, *Google's Big Bet on the Mobile Future*, N.Y. TIMES: DEALB%K (Aug. 15, 2011, 9:47 PM), http://nyti.ms/z2PB9d ("Google made a $12.5 billion bet on Monday that its future—and the future of big Internet companies—lies in mobile computing, and moved aggressively to take on its arch rival Apple in the mobile market.").

19. *See* Gross, *supra* note 11.

locations with virtual data to assist tech-savvy shoppers will gain a competitive advantage.[20] With the advent of smartphone technology, the importance and depth of adoption of Mixed Reality applications far outstrips that of pure virtual reality applications.

The second gap lies in the legal literature of pervasive computing ("PerC"). PerC is the predicted future embedding of computer chips into the physical environment. In the future, PerC theorists predict that there will be microprocessors—such as radio frequency identification ("RFID") chips—in credit cards, shoes, toasters, walls, ceilings, and refrigerators.[21] But the PerC literature has missed the mark because data tagging of realspace has preceded PerC by at least twenty years.[22] While implantation of chips into people and the environment is still in its infancy, Yelp, Google Latitude, Hidden Park, Parallel Kingdom, and other mixed reality applications are already here, and from these applications will come the next wave of great internet successes.[23] Thus, the PerC literature assumes a legal environment based on the prevalence of physical objects that transfer information embedded throughout our everyday lives, when the reality is that technology has developed in a different way, and much more quickly. This reality—that of Mixed Reality here and now—has not been addressed in the legal literature discussing PerC.

While the World Wide Web revolutionized human knowledge by linking it together, indexing it, and making it searchable, today a far greater revolution is underway: the real world itself is becoming hyperlinked and indexed. One example of hyperlinking the real world are quick response codes ("QR-codes")—tags in the real world that can either link to a website or contain information about the location or object near which they are

20. *See* Chris Crum, *Is Augmented Reality the Future of E-Commerce? eBay Lets You Virtually Try On Sunglasses*, WEBPRONEWS / TECH. (Jan. 7, 2011, 2:15 PM), http://www.webpronews.com/is-augmented-reality-the-future-of-e-commerce-2011-01 ("Augmented reality could potentially be the biggest thing in e-commerce since the search engine.").

21. *See* Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93, 98 n.10, 99 (2005) ("What we can expect [if active RFIDs stood in our shoes], then, are networks of miniaturized, wirelessly interconnected, sensing, processing, and actuating computing elements kneaded into the physical world.").

22. *See* Nancy J. King, *When Mobile Phones Are RFID-Equipped—Finding E.U.-U.S. Solutions To Protect Consumer Privacy and Facilitate Mobile Commerce*, 15 MICH. TELECOMM. & TECH. L. REV. 107, 112 (2008) (discussing the use of RFID tags in mobile phones and RFID readers while also discussing location-based services). RFID chips are present but are being used as support tools for mixed reality apps.

23. *Id.*; *see also* Lesley Fair, Fed. Trade Comm'n, *Information Technology Law Institute 2011: Navigating the New Risks in Mobile Technology, Social Media, Electronic Records and Privacy*, 1043 PLI/Pat 417, 483 (Apr.–May 2011) (noting that the FTC convened to explore the emergence of RFID only in 2004).

found. Once a smartphone recognizes the QR-code, it provides the user with access to websites, free e-books, streaming videos, or even three-dimensional ("3-D") overlays onto the physical reality perceived by the smartphone user through the device.

Figure 1: QR-Code Linking to This Article on BTLJ.org

Thus, the Mixed Reality revolution is already happening. The real world is already alive and crawling with attached data. Data is routinely attached to real-world people, places, and things, and mobile devices permit users to experience this local data in the place to which it is attached. Well in advance of the advent of the pervasive computing world, data tagging has already hyperlinked and virtualized the real world—our world today.

The remainder of this Article proceeds in four Parts. Part II explores and defines Mixed Reality technologies and demonstrates the gaps in the legal literature on virtual worlds and the legal literature on pervasive computing. Part III analyzes the legal implications of the ongoing extension of virtual governance regimes into realspace and projects future trends. Part III also anticipates several legal problems including a Mixed Reality land rush[24] similar to the domain name rush of the late 1990s,[25] the advent of new forms of cyberdefamation or reputation poisoning, and dignitary harms based on false information propagated through Mixed Reality applications.[26] Part IV modestly proposes that as real and virtual worlds converge, the best available analogy for governing Mixed Reality are the background principles of the common law, not the law of online intellectual property licensing. Part V offers a brief conclusion.

24. *See* CHEN, *supra* note 6, at 20, 31 (discussing the mobile app store as a digital gold rush, which is a strong indication that the Apple App Store is still in its infancy and is the sequel to the dot-com boom).

25. *See* Jacqueline D. Lipton, *Bad Faith in Cyberspace: Grounding Domain Theory in Trademark, Property, and Restitution*, 23 HARV. J.L. & TECH. 447, 448–49 (2010) (detailing the origins of the domain name rush and the negatives that ensued such as cybersquatting); *see also* Anupam Chander, *The New, New Property*, 81 TEX. L. REV. 715, 724 (2003) (discussing the domain name "land rush").

26. *See* Reit v. Yelp!, Inc., 907 N.Y.S.2d 411 (Sup. Ct. 2010) (discussing claim by dentist for defamation and deceptive acts and practices against Yelp).

II. MIXED REALITY

This Part places Mixed Reality experiences on a continuum between virtual and real worlds. It first describes the various technologies and techniques for creating Mixed Reality experiences and then offers a more developed taxonomy for describing the various types of experiences that the technology can create.

A. THE TECHNOLOGY

Mixed Reality is exactly what it sounds like—the mixing of "virtual" and "actual" reality.[27] The core of Mixed Reality is not new. The central element of Mixed Reality is the tying of data to an anchor in the real world, be it a person, geographic location, or structure. Some early examples of data tying are gossip circles in medieval villages or land records that indicated property ownership. In gossip circles, the act of gossiping "tagged" a person with information about that person. Land records—although much less accessible in medieval times—similarly linked a person to an ownership interest in property. Today the same type of data can be tied to a person or property through virtual technology. For example, circles in Google+[28] now give information about a person, much like a medieval gossip circle.[29] Mobile applications that list land ownership and property values when the user snaps a photo of a house with a smartphone now link that information to the property.[30] In both of these examples, information that had always been tied to an object (a person's reputation through gossip, or real estate ownership through land records) is now being made available seamlessly through technology. What makes Mixed Reality significant is the scale of this new data-enriched realspace.

One new aspect that Mixed Reality introduces is the combination of mobile computers with geotagged data and the extent to which this

27. *See* Paul Milgram & Fumio Kishino, *Taxonomy of Mixed Reality Visual Displays*, E77-D IEICE TRANSACTIONS ON INFO. & SYS. 1321, 1322–29 (1994), *available at* http://ci.nii.ac.jp/naid/110003209335.

28. *See A Quick Look at Google+*, GOOGLE, http://www.google.com/+/learnmore/ (last visited Feb. 18, 2012).

29. Google+ profiles show other users whom the profile owner has placed in his "circles" and facilitates the sharing of the owner's daily life (depending on how frequently he uses Google+). Medieval gossip circles would have similarly indicated whom someone knew, and would have also revealed the goings-on of the person's life. Thus, both have the same fundamental function; the difference now is that this information is readily accessible through a smartphone, whereas one would have to actually sit in a gossip circle to gain this information.

30. *See, e.g.*, ZipRealty, *ZipRealty Real Estate*, APPLE ITUNES, http://itunes.apple.com/us/app/ziprealty-real-estate/id340513671 (last updated Jan. 30, 2012).

combination is a part of our everyday lives. Through mobile devices, users see data that is tied to particular places, objects, or people that they encounter.[31] Smartphone technology and other miniaturized computers permit a more mobile and interactive experience with our surroundings.[32] Coupled with the growth in mobile computing is the growth in Mixed Reality applications. Now, a husband who goes shopping can peer through his smartphone camera at a product and immediately see tagged locations of local competing stores with better prices.[33] A lost tourist in London can look through her smartphone and see virtual arrows overlaid on top of the real world that guide her to the nearest Underground station.[34] A potential Boston bar-crawler can use his cell-phone to examine the virtual tags that other patrons have left behind describing the best drinks served at a given hotspot.[35] Parents can install geolocation devices in cars that mentor overzealous teenage drivers and provide parents with instant information about their teen's driving.[36] In short, Mixed Reality takes computing out from behind the desk and into the real world.[37]

As we do so, what matters is not that computers are everywhere, but that they are with people. Given that a person can carry a smartphone in her pocket and access data that other people have tied to a given location, object, or person, people now move through a world augmented with data tags.[38] In the same way that people can click the "like" button on a Facebook

31. *See In re* Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993 (*Data Traffic Growth*), 25 FCC Rcd. 11407, 11412–25 (2010); *id.* ¶ 4 ("Data traffic has grown significantly, due to the increased adoption of smartphones and data consumption per device."); *see also The State of Mobile Apps*, NIELSENWIRE (June 1, 2010), http://blog.nielsen.com/nielsenwire/online_mobile/the-state-of-mobile-apps/ ("21% of American wireless subscribers have a smartphone at Q4 2009, up from 19% in the previous quarter and significantly higher than the 14% at the end of 2008.").

32. *See Data Traffic Growth*, 25 FCC Rcd. 11407, ¶ 4 ("As of the end of 2008, 90 percent of Americans had a mobile wireless device.").

33. *See, e.g.*, SHAPE Servs., *Barcode Reader*, APPLE ITUNES, http://itunes.apple.com/us/app/barcode-reader/id340825499 (last updated June 9, 2011).

34. *See* acrossair, *Nearest Tube*, APPLE ITUNES, http://itunes.apple.com/app/nearest-tube/id322436683 (last updated July 16, 2010).

35. *See* GoTime, *Happy Hours*, APPLE ITUNES, http://itunes.apple.com/us/app/happy-hours/id303814652 (last updated Oct. 17, 2011).

36. *See In-Car Teen Mentoring Device*, AM. NAT'L PROP. & CAS. CO., http://www.anpac.com/DriveSmart/WhatIsDriveSmart/Mentoring/default.aspx (last visited Feb. 18, 2012).

37. *See Data Traffic Growth*, 25 FCC Rcd. 11407, ¶ 4 ("Data traffic has grown significantly, due to the increased adoption of smartphones and data consumption per device.").

38. *See* CHEN, *supra* note 6, at 4 ("Data has become so intimately woven into our lives that it's enhancing the way we engage with physical reality."); *see also, e.g.*, SHAPE Servs., *supra* note 33 (describing the *Barcode Reader* app as permitting the user to instantly compare prices by scanning items in a physical store).

comment, they can now click the "like" button for a restaurant, or a colleague, or a neighborhood. Popular apps like Yelp and Foursquare have already turned this practice into a runaway business model.

Thus, data tagging—the tying of information to a specific geographical location or realspace anchor—not embedded computing, is driving the virtualization of realspace.[39] Data tagging can be done in a number of different ways. Global Positioning System ("GPS") tagging, other Location Based Services, tagging through what will be called Identification Services ("IDS"), mobile tagging, and Near Field Communication ("NFC") are all forms of data tagging. Each of these data tagging methods adds to Mixed Reality in a unique way.

By far the most common data tagging method is GPS data tagging (colloquially, "geotagging").[40] A GPS-enabled smartphone knows to overlay a given reputation bar on top of the local eatery because a global positioning system has identified the location of the restaurant.[41] When the smartphone knows its longitude and latitude, it can display information relevant to that location. A simple example and common application of GPS tagging comes from the world of outdoor hiking.[42] Geocaching has become an international phenomenon.[43] A geocacher is a hiker who hides a small object for other hikers to find by using a GPS tag left by the original geocacher. With their smartphones or GPS device, hikers find these objects in the real world by relying on the data that is tagged to the physical location of the geocache. They can then log their visits online with the rest of the tech-savvy hikers that located the geocache before. Geocaching takes a simple activity like

39. *See* Kang & Cuff, *supra* note 21; *see also* Mark Weiser, *The Computer for the Twenty-First Century*, 265 SCI. AM. 94, 104 (1991) ("Already computers in light switches, thermostats, stereos and ovens help to activate the world. These machines and more will be interconnected in a ubiquitous network."). This literature is either behind the times, or has managed to identify the new trend, that data tagging is driving the virtualization of realspace.

40. *See* Ian Austen, *Pictures, with Map and Pushpin Included,* N.Y. TIMES (Nov. 2, 2006), http://www.nytimes.com/2006/11/02/technology/02basics.html (defining geotagging in the photography context as a technology "which, broadly speaking, is the practice of posting photos online that are linked to Web-based maps, showing just where in the world the shutter was pressed"); *see also* Andrew Adam Newman, *Appearing Virtually at a Store Near You . . .* , N.Y. TIMES, Jan. 19, 2011, at B9.

41. *See* AB InBev, *Stella Artois—Le Bar Guide*, APPLE ITUNES, http://itunes.apple.com/us/app/id335624129 (last updated June 29, 2010).

42. *See* Groundspeak, Inc., *Geocaching—The Official Global GPS Cache Hunt Site*, GEOCHACHING, http://www.geocaching.com/ (last visited Feb. 18, 2012) (detailing the user base at "1,648,021 active geocaches and over 5 million geocachers worldwide").

43. *See* Mark Couhig, *Geocaching Is Catching On*, SEQUIM GAZETTE (Dec. 15, 2010), http://www.sequimgazette.com/news/article.exm/2010-12-15_geocaching_is_catching_on.

hiking, augments it with data tagged to real-world physical locations, and transforms it into a hidden world of treasure hunting.[44]

Due in part to the success of GPS, it has been coupled recently with another type of data tagging, sometimes called Identification Services.[45] The difference between GPS and IDS is that, while GPS relies on GPS coordinates, IDS relies on some visual or audio cue within the local environment, be it a corporate logo, a face (for facial recognition software), or even a fragment of a musical tune (as in the case of the popular Shazam music-identification app). The real and virtual worlds connect through the smartphone's lens or audio pickup.[46] This requires the user to be in front of the real world cue. For instance, a user must be in front of a Starbucks and view the Starbucks logo through the camera lens before the application will "check in" using an IDS.

Mobile tagging also hyperlinks reality. While closely related to IDS it relies on barcodes or other machine-readable codes to retrieve virtual information. Mobile tagging, such as QR-codes, is more involved than IDS because information is not tagged to a visual or audio cue but rather embedded within the barcode or image itself. The mobile tag contains the code that creates the virtual experience, whereas IDS merely identifies the point where information is tagged. Mobile tag data can be a web address, a connection to a wireless network, a free e-book, a Sudoku puzzle, or even an animated graphic of a tank bursting through the wall.[47] The most prevalent examples of mobile tagging are QR-codes that act as a link to an online web presence, but there are numerous other applications.[48]

---

44. *See* Groundspeak, Inc., *supra* note 42; *see also* bulpadok, *The Hidden Park*, APPLE ITUNES, http://itunes.apple.com/us/app/the-hidden-park/id314518306 (last updated Mar. 5, 2010).

45. *See* Bryan Pardo, *Finding Structure in Audio for Music Information Retrieval*, 23 SIGNAL PROCESSING MAG., May 2006, at 126, 127 (referring to Shazam and similar products as "identification services"); Chris Crum, *Augmented Reality + Location = The Holy Grail for Marketers?*, WEBPRONEWS (Feb. 28, 2011), http://www.webpronews.com/augmented-reality-plus-location-the-holy-grail-for-marketers-2011-02 (discussing how adding a visual element to GPS-based services makes consumer engagement much stronger than simple GPS-based applications).

46. *See* SHAZAM, http://www.shazam.com (last visited Dec. 8, 2011) (featuring a music identification service).

47. *See* Andy Vuong, *Wanna Read That QR Code, Get the Smart Phone App*, DENVER POST (Apr. 18, 2011), http://www.denverpost.com/business/ci_17868932.

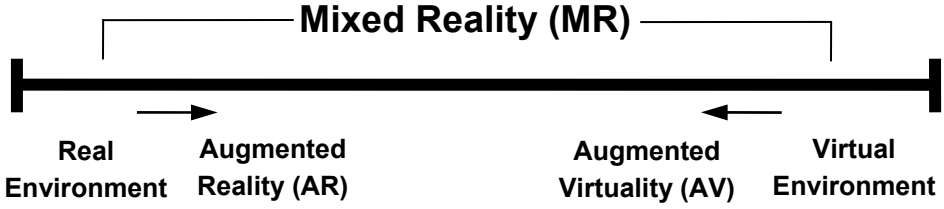
48. Other types of two-dimensional barcodes developed include DataMatrix, Cool-Data-Matrix, Aztec, Upcode, Trillcode, Quickmark, Shotcode, mCode, Beetagg, and Microsoft's new Microsoft tag.

Near Field Communication[49] is yet another form of data tagging. With NFC, the application is closer to the vision of the pervasive computing literature. NFC relies on computer chips embedded in the environment or objects that are able to communicate information to one another via extremely short range radio fields (separated by mere meters). An example of NFC technology might be an application that allows a mobile device to function as a credit card and that could be waved near a receptor in a store in order to be "swiped." However, because NFC requires two sets of embedded chips in order to function, it is a far less commonly used method of geolocating data than GPS, IDS, or mobile tagging.

B. A TAXONOMY OF EXPERIENCES ALONG THE REALITY-VIRTUALITY CONTINUUM

As will be seen, *infra*, understanding where a given communication lies on the continuum between virtual and real will be of some help in understanding what legal analogy should apply to a given phenomenon. This Section provides a practical set of terms for discussing the technology. As a baseline, the Article uses Milgram's Reality-Virtuality continuum ("RV continuum") as one potentially useful scheme for measuring out the steps from the virtual to the real.[50] As can be seen below, the term "Mixed Reality" sometimes refers to the various experiences between fully virtual and fully real. This Section therefore builds out the continuum to provide a more complete picture of the range of experiences offered by virtualization technologies and explains how Mixed Reality—as used in this Article—is used much more narrowly than the broad concept of Mixed Reality as a description of experiences on the RV continuum.

Figure 2: Milgram's Reality-Virtuality (RV) Continuum[51]



49. *See About NFC*, NFC FORUM, http://www.nfc-forum.org/aboutnfc/ (last visited Aug. 15, 2011).

50. *See* Fumio Kishino et al., *Augmented Reality: A Class of Displays on the Reality-Virtuality Continuum*, 2351 PROC. SPIE 282, 283 (1994), *available at* http://spiedigitallibrary.org/proceedings/resource/2/psisdg/2351/1/282_1 (identifying Milgram's Reality-Virtuality Continuum).

51. Milgram & Kishino, *supra* note 27, at 1321.

Mixed Reality occupies the space between virtual worlds and realspace.[52] Like any in-between technology, Mixed Reality is defined both by what it is and what it is not. The first problem in defining mixed reality is how to keep a definition from spilling over into generalized network technologies. Overuse of the word "virtual" exacerbates this challenge.[53] Virtual has come to mean anything electronic.[54] Thus, without care, it is easy to expand the definition of Mixed Reality to include almost all data used by people in the real world—that is, all data. A definition that broad is unlikely to be of much use.

A more accurate definition characterizes a virtual object or experience as a digital representation of something that we would typically expect to find in the real world.[55] Mixed Reality then re-injects or repositions that virtual object back into our real world experience. For example, consider a table. One can build a virtual table in a video game or virtual world, but it does not appear in the real world. But with Mixed Reality technologies, one can experience a virtual table in the real world; one can see an image of it manifested in the real world through mobile computing technologies and perhaps decorate it with virtual flowers as well. A table is an overly simple example but the point remains clear: Mixed Reality involves the injection of virtual places, objects, experiences, or other data into real-world contexts.

The second problem with defining Mixed Reality is how to locate Mixed Reality in the range of technologies from virtual worlds to pervasive computing. Over-breadth is again a real risk. Simply defining Mixed Reality as any application of mobile or pervasive computing, when coupled with the "virtual" fallacy above, would mean that one might classify nearly any mobile phone app as a Mixed Reality experience. In fact, the term means something quite specific: it means the projection of virtual objects and experiences into our physical lives.[56]

---

52. *See* Robin Fretwell Wilson, *Sex Play in Virtual Worlds*, 66 WASH. & LEE L. REV. 1127, 1131–32 (2009) ("These 'augmented reality' technologies push virtual experiences and object down into real space, erasing the boundary between the virtual world and the real world."); *see also* Marc Jonathan Blitz, *The Freedom of 3D Thought: The First Amendment in Virtual Reality*, 30 CARDOZO L. REV. 1141, 1144 (2008) (noting that engineers "erase the perceptual barriers" with mixed reality by "mak[ing] illusory three-dimensional people and objects spring up in the more familiar settings in front of us").

53. *See* M. Scott Boone, *Ubiquitous Computing, Virtual Worlds, and the Displacement of Property Rights*, 4 I/S: J.L. & POL'Y INFO. SOC'Y 91, 108–09 (2008).

54. *Id.*

55. *See* Milgram & Kishino, *supra* note 27, at 1324–25; *see also* Boone, *supra* note 53, at 109.

56. *See* Milgram & Kishino, *supra* note 27, at 1322 ("[T]he most straightforward way to view a Mixed Reality environment, therefore, is one in which real world and virtual world objects are presented together within a single display . . . .").

Mixed Reality and PerC fundamentally differ with respect to where data is stored and processed.[57] Pervasive computing implies that the processing power is embedded in objects all around the user. Instead of tagging data on the cloud to virtual points in the real world, PerC stores and processes this information in computers in the physical environment around you. Unlike PerC, Mixed Reality utilizes data stored on the cloud globally but accessed locally; it is tied to real places, people, or objects through wireless connectivity and location based services. Mixed Reality and cloud computing go hand-in-hand.[58] With these definitions in mind, the following Sections explore the broader range of experiences that virtualization technologies offer and attempt to locate Mixed Reality technologies within that spectrum.

1. Virtual Reality

One end of the virtualization spectrum is marked by pure virtual reality. Virtual reality is virtualization at its most profound because the goal is to immerse the user in a virtual environment as completely as possible.[59] Virtual reality is the "goggles and gloves" technology that attempts to capture every sensation possible.[60] Due to bandwidth and processor constraints, as well as the required gear that tends to be expensive, cumbersome, and complex, the technology has not progressed far past the experimental stage or the occasional appearance in movies like *Tron*, *The Matrix*, or *Lawnmower Man*.[61] The technology is visually interesting and full virtual reality is often the first thing to spring to the layman's mind when contemplating virtual experiences.

Yet full goggles-and-gloves reality does not capture the current flowering of virtual experiences—known in somewhat passé technological parlance as "Web 2.0." The reason is simple: the current digital revolution is social, not

57. *See* Eric Taub, *Storing Your Files Inside the Cloud*, N.Y. TIMES (Mar. 2, 2011), http://www.nytimes.com/2011/03/03/technology/personaltech/03basics.html ("Cloud backups are appealing for another reason: as computing becomes more mobile—on laptops, tablets and smartphones—you need to have reliable access to the data anywhere over an Internet connection.").

58. *See id*; *see also* Edward Lee, *Warming Up to User-Generated Content*, 2008 U. ILL. L. REV. 1459, 1500–01 (discussing that cloud computing is a major component of Web 3.0 in which the Internet converts traditional desktop-based applications into web-based applications that run off of massive amounts of data on remote servers).

59. *See* Milgram & Kishino, *supra* note 27, at 1321 ("The conventionally held view of a *Virtual Reality* . . . environment is one in which the participant-observer is totally immersed in, and able to interact with, a completely synthetic world.").

60. *See* Jonathon W. Penney, *Privacy and the New Virtualism*, 10 YALE J.L. & TECH. 194, 220 (2008) (discussing virtual reality and the two-way interaction between virtual technology and the user).

61. *See id.* at 220 ("The amount of information processing power necessary for such seamless interaction has not been developed and might never be.").

technological.[62] Virtual experiences matter because they are shared,[63] not because they utilize exceptionally rendered 3-D computer graphics.[64] There exists a sweet spot where the technology is simple enough to be widely adopted, yet complex enough to offer a compelling virtual experience.[65] This explains why smartphones—not virtual reality goggles and gloves—are the current carriers of Mixed Reality experiences. The reality is that more people will have these shared experiences if they are enabled by readily available and relatively inexpensive mobile devices. Shared experiences, not completely immersive experiences, are driving the current push into the most successful mobile apps.[66]

Consumers have clearly indicated that they seek socially rich virtual experiences. But mobile computing depends on smaller computers.[67] Thus, virtual worlds have become simpler, isometric social spaces that can be effectively accessed through a smartphone, rather than the fully-rendered immersive 3-D spaces that require bleeding edge (and large) computers.[68] Mobile means smaller, and smaller means more social and less graphically intensive.[69] Thus, in considering virtual worlds technologies in the following

62. *See* Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 480–81 (2010) (referencing the social nature of Web 2.0, for example the expanded options for people to magnify their voice through blogs, wikis, social networks, and MMOGs).

63. *See* BENJAMIN DURANSKE, VIRTUAL LAW: NAVIGATING THE LEGAL LANDSCAPE OF VIRTUAL WORLDS 12 (2008) ("Most people who enter virtual worlds do so to interact with other users. This makes virtual worlds highly social spaces . . . .").

64. *See* Edward Castronova, *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier* 6 (CESifo, Working Paper Series No. 618, 2001), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=294828 (noting that successful virtual worlds combine 3D computer graphics with "chat-based social interaction systems"). The graphics in the games mentioned are not part of complex, full-immersion virtual reality experience, but rather they are experienced merely through one's computer.

65. To see how simple graphics interfaces in highly social games can be more appealing than less socially-oriented games with high end graphics, compare Zynga, *Farmville*, FACEBOOK, http://www.facebook.com/FarmVille (last visited Aug. 3, 2011) (identifying 34,070,983 monthly active users), with Press Release, Blizzard Entm't, World of Warcraft Subscriber Base Reaches 12 Million Worldwide (Oct. 7, 2010), http://us.blizzard.com/en-us/company/press/pressreleases.html?id=2847881 (stating a 12 million subscriber population).

66. *See The State of Mobile Apps*, *supra* note 31 (highlighting that Facebook is the most popular app on the iPhone and BlackBerry, and the second most popular on the Android platform).

67. *See* REZA B'FAR, MOBILE COMPUTING PRINCIPLES: DESIGNING AND DEVELOPING MOBILE APPLICATIONS WITH UML AND XML 5, 12–13 (1st ed. 2005) (describing the evolution of mobile computing).

68. *See* Zynga, *supra* note 65 (describing a popular virtual world game, *Farmville*, which is browser-based and does not require high-performance graphics hardware and computing power).

69. *See* B'FAR, *supra* note 67, at 6, 13.

Section, this analysis includes those highly social but graphically simple virtual worlds that are based on mobile and browser technology.

2. Virtual Worlds

A virtual world is a persistent, interactive, avatar-mediated, simulated 3-D space (much like virtual reality), but with more social and fewer immersive features than pure virtual reality.[70] Virtual worlds facilitate social interaction and enrich it with a shared graphical context.[71] At the nexus between social networking technology and 3-D game environments, virtual worlds follow a very different aesthetic from virtual reality. Virtual worlds do not place the user directly "inside" a virtual environment. Rather, virtual worlds often make use of avatars—characters viewed in the third person that represent the players in the virtual world. Avatars permit an increased range of interaction within the world by indicating a user's focus of attention and that of other players.[72] Judge Posner illustrated the unique ability for avatars to convey user focus when he conducted an interview in the virtual world of Second Life entirely through his virtual avatar.[73]

Although graphically engaging and immersive, virtual worlds continue to utilize the lower end of graphics capabilities in order to capture as many users as possible. Some virtual worlds remain graphically rich and only run on high-end computers, but the number of players in such worlds has been rapidly outstripped by browser-based games, such as those running on Adobe's Flash platform. Thus tension exists between the immersiveness of the environment and accessibility to large numbers of users, many of whom may not have high-end computers.[74]

---

70. *See* Castronova, *supra* note 64, at 5–6; *see also* DURANSKE, *supra* note 63, at 2.

71. *See* DURANSKE, *supra* note 63, at 12.

72. *See* Penney, *supra* note 60, at 221 (detailing that avatars are not only a visual representation of the user in the virtual world where the user has full control over the avatar's appearance and actions, but often, the avatar becomes the person in the virtual world). An example is a recent lecture given by Professor Lastowka and this author at the Governance in Virtual Worlds Conference at the ASU Sandra Day O'Connor Law School. Participants attended with their own avatars and were able to interact with the professors' avatars. The avatars served as a means to convey social information: social focus, gaze, proximity, experience, and engagement are all conveyed via the avatar. Although avatar-mediated discourse is not as immediate as person-to-person conversation, the use of avatars as markers for social discourse permits a feeling of increased social engagement despite the limitations of the virtual environment.

73. *See* UChicagoLaw, *Judge Posner (or at Least His Avatar) Talks to Second Life*, U. CHI L. SCH.: FACULTY BLOG (Nov. 29, 2006, 10:38 AM), http://uchicagolaw.typepad.com/faculty/2006/11/judge_posner_or.html.

74. *See* Joshua A.T. Fairfield, *The Magic Circle*, 11 VAND. J. ENT. & TECH. L. 823, 838 (2009).

The trend towards ease of access has led to the popularity of several flash games, in particular, Zynga Networks' Cityville and Farmville, which run on Facebook.[75] These games have exploded both in the traditional computer setting and in mobile computing with smartphones and tablet PCs. These games demonstrate the principles outlined in the following Sections: they are graphically simple and run over social networks.

3. Augmented Virtuality

Augmented virtuality is the point at which realspace begins to enter virtual worlds. Virtual worlds—such as Second Life—include the capacity to import real events into the virtual space for virtual world denizens to view. A real-world presidential debate can be imported and streamed live to those virtual world denizens.[76] Avatars can sit in an auditorium within an entirely virtual environment and watch events unfolding in the real world.

Google Maps and Microsoft's Bing Maps provide other examples. Both now include a "drill down to reality" function.[77] Whereas before a Google Maps or Bing Maps user might have ended her journey with a real world photograph of her destination (taken by the Google Streetview cars or geographically tagged photos taken by passers-by), the currently evolving functionality augments the virtual world with a drill down to a live camera view. Thus the drill down of a motorist using Bing Maps might be to a traffic camera, or the drill down of a remote viewer might be to a handheld camera that is currently active in the location. One example of this technology is the subject of Blaise Agüera y Arcas's TED talk, in which he demonstrated the ability to drill down all the way from a virtual world into realspace real-time live handheld cameras.[78] These technologies permit users of virtual worlds access to the real world. In so doing, they begin to mix even more reality into the virtual environment.

---

75. *See* Douglas Macmillan, *Zynga and Facebook. It's Complicated*, BLOOMBERG BUSINESSWEEK (Apr. 22, 2010, 5:00 PM), http://www.businessweek.com/magazine/content/10_18/b4176047938855.htm (detailing the close relationship between Zynga and Facebook).

76. *See Presidential Debate Festivities in Second Life*, GAME POL. (Sep. 29, 2008), http://www.gamepolitics.com/2008/09/29/presidential-debate-festivities-second-life.

77. *See* John D. Sutter, *Bing Wows Crowd with Live-Video Maps*, CNN SCITECHBLOG (Feb. 12, 2010, 4:50 PM), http://scitech.blogs.cnn.com/2010/02/12/bing-wows-crowd-with-live-video-maps/ (discussing the live-feed feature in Bing Maps); *Viewing Layers—Maps Help*, GOOGLE, http://support.google.com/maps/bin/answer.py?hl=en&answer=144359 (last visited Feb. 18, 2012) (stating that one of Google Map's viewing layers contains live images from webcams around the world).

78. *See Blaise Aguera y Arcas Demos Augmented-Reality Maps*, TED (Feb. 2010), http://www.ted.com/talks/blaise_aguera.html (discussing the work of Microsoft with Bing Maps, the integration of cartography, imagery, and user content to augment realspace).

4. Mixed / Augmented Reality

This leads to the narrow definition of Mixed Reality within the RV continuum. Although the term "Mixed Reality" can broadly encompass all stages of data-enriched real or virtual environments (i.e., the entire RV continuum), for purposes of this Article Mixed Reality represents a narrow point in the spectrum where near-field technology,[79] geolocation services,[80] identification services, mobile tagging, and other data tagging techniques enrich the real world with virtual data through the use of technology. This technology is also sometimes called "Augmented Reality."

The November 2009 issue of Esquire Magazine contains one example of Mixed Reality. It contained Mixed Reality tags such that the magazine cover and several internal advertisements contained virtual elements that only appeared when the magazine was viewed through a computer or smartphone camera.[81] Another Mixed Reality application called Hidden Park permits children to see fantastic dragons, trolls, and fairies when specific areas of the park are viewed through a smartphone.[82] A child might look at a tree through the smartphone camera and see a goblin face peering out, or a child might look over a field to see elves dancing. Beyond opening up fantastical opportunities for play, these Mixed Reality apps have tremendous potential as educational tools.[83] The combination of an app like wikitude[84]—one of the most popular augmented reality applications—and Hidden Park may fulfill a goal of many parents and teachers: getting kids to enjoy learning. With technology that provides an interactive experience, otherwise boring topics like math or history may become more social, fun, and educational. Children might be more likely to learn math if it involved counting virtual dinosaurs in the park and might be more likely to learn American history with a virtual

79. *See* King, *supra* note 22, at 211 (discussing Near Field Communications ("NFC") technologies and how they rely on RFID chips in mobile handsets, the software on the mobile handsets, and how NFC will deliver mobile advertising and other location-based services).

80. *See* Wendy A. Adams, *Intellectual Property Infringement in Global Networks: The Implications of Protection Ahead of the Curve*, 10 INT'L J.L. & INFO. TECH. 71, 89 (2002) (identifying geolocation services as referential databases that are arguably inferior to GPS technologies).

81. *See* Shira Ovide, *Esquire Tries Out Digital Reality*, WALL ST. J., Oct. 29, 2009, at B10.

82. *See* bulpadok, *supra* note 44.

83. *See* Mark Sutton, *Soar Valley College: Augmented Reality in the Classroom*, GUARDIAN (London) (Dec. 2, 2010), http://www.guardian.co.uk/classroom-innovation/video/soar-valley-college (discussing a professor's successful effort to interact with underachieving students by using an augmented reality experience to engage students with the solar system).

84. *See* Mobilizy GmbH, *Wikitude*, APPLE ITUNES, http://itunes.apple.com/us/app/wikitude/id329731243 (last updated June 29, 2011).

world overlay of revolutionary-era Boston life.[85] This blending of education with fun using technology is not new. The difference now is that mobile computing combined with data tagging and the resulting virtually enriched realspaces are far more social and dynamic than these earlier media.

Mixed Reality applications sit at the midpoint of the RV continuum. They are grounded in real objects and space but augment those objects or places with computer-generated data. For example, some greeting cards now contain a virtual enhancement.[86] The card includes a code that the sender can customize with an animated message and the receiver can scan it with a cell phone or web-cam and see the cartoon. The computer layers the 3-D representation onto the object. Often identifying which image to display does not even rely on server architecture. Rather, in many cases, the augmented reality object contains a mobile tag that provides sufficient data for the computer to render a three dimensional image.[87] In these instances the real world mobile tag provides the data for the virtual application; the mobile tag augments realspace with data that links directly to that physical printed code.

5. "Reality+"

The final point on this continuum is Reality+. I borrow and use the term reality plus—rather than simple reality—because realspace has always been enriched by information ever since the first fisherman told the second which fishing holes were especially good.[88] What is worth noting about realspace is that we have always augmented reality with crude data tagging. Maps and charts have served as crude data tagging devices tied to latitude and longitude. The revolution is in the accuracy, availability, and accessibility of such markers[89] and of the propagation of information on a global scale.

---

85. *See, e.g.*, *Dinosaur Games*, PBS KIDS, http://pbskids.org/games/dinosaurs.html (last visited Oct. 15, 2011) (providing dinosaur-themed games for children to learn various skills and subjects).

86. *See Webcam Greetings*, HALLMARK, http://www.hallmark.com/online/webcam-greetings.aspx (last visited Aug. 8, 2011).

87. *See id.* The example above includes a feature where you can print out a free sample from Hallmark complete with the mobile tag. If you simply hold the card up to a webcam, your image pops to life.

88. *See* Mark Burdon, *Privacy Invasive Geo-mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws*, 2010 U. ILL. J.L. TECH. & POL'Y 1, 4 n.62 (explaining *Fishing Lake Map*, an app that provides geotagged updates on fishing holes).

89. *See* Nick Bilton, *Augmented Reality on Your Phone*, N.Y. TIMES BITS (Dec. 20, 2010, 3:40 PM), http://bits.blogs.nytimes.com/2010/12/20/augmented-reality-on-your-phone/ (identifying, based on a recent report from Forrester research, that augmented reality apps will become an integral, and common, part of using a mobile phone); *see also* Thomas Husson, *Mobile Augmented Reality: Beyond the Hype, a Glimpse into the Mobile Future*, FORRESTER: THOMAS HUSSON'S BLOG (Dec. 20, 2010), http://blogs.forrester.com/thomas_husson/10-12-

It is important to remark on what reality has always shared with information-enriched environments because of how law works. Much of law is a primitive form of augmenting real spaces and objects with data tags. Think about the title recording system for land. Land is not naturally divided into three-acre parcels. An entry in a paper or (increasingly) an electronic database tags specific land as "yours." Property is, therefore, a form of information-enriched geotagging.[90] Like all of law, property is a consensual fiction based on information-enriched reality.

C. THE GAP BETWEEN THE LEGAL LITERATURES OF VIRTUAL WORLDS AND PERVASIVE COMPUTING

Having discussed the technology and terminology of Mixed Reality, the Article now turns to the two closest legal literatures: virtual worlds and pervasive computing. There is an extensive legal literature on virtual worlds and a less extensive, but still fascinating, legal literature on pervasive computing. This Section examines the gaps within and between these literatures and then demonstrates that a developed legal theory of Mixed Reality fills those gaps.

1. The Legal Literature of Virtual Worlds

Legal academics have written several hundred articles focusing on virtual worlds in past years.[91] This rich literature has addressed issues including virtual property,[92] democracy,[93] control over land,[94] the use of contracts to govern virtual worlds,[95] the impact of policing and surveillance in virtual worlds,[96] the taxation of virtual currency,[97] and the sales of virtual goods.[98]

20-mobile_augmented_reality_beyond_the_hype_a_glimpse_into_the_mobile_future (stating that while augmented reality is not new, it is moving to mobile platforms). Although augmented reality is currently overhyped due to unrealistic expectations, it is growing rapidly and drivers for growth are in place.

90. *See id.*; Burdon, *supra* note 88, at 7–9 (discussing the expanded use of GPS, location-oriented, and function-oriented geo-mashups which overlay information onto a map of the real world). This use of software to tag information, such as a new cycling or running route, is substantially the same as the overlay of property boundaries upon realspace.

91. For a nonexhaustive list of virtual worlds literature, see sources cited *supra* note 15.

92. *See* Joshua A.T. Fairfield, *Virtual Property*, 85 B.U. L. REV. 1048 (2005).

93. *See* Beth Simone Novek, *Introduction: The State of Play*, 49 N.Y.L. SCH. L. REV. 1 (2005); *see also* Jankowich, *supra* note 15.

94. *See* Jankowich, *supra* note 15, at 207–08 (discussing the use of licensing by Linden Labs and Sony to control property in virtual worlds).

95. *See* Fairfield, *supra* note 8.

96. Joshua A.T. Fairfield, *Escape into the Panopticon: Virtual Worlds and the Surveillance Society*, 118 YALE L.J. POCKET PART 131 (2009).

97. *See* Camp, *supra* note 15.

98. *See* Michael H. Passman, *supra* note 15.

The articles share an intuition that virtual worlds are not only an interesting and novel technology, but that they also represent a compelling example of the law's development through the common law process.[99] As new communities encounter new technologies, they first develop norms, then they develop practices that are adopted by courts and eventually the practices are codified by statute.[100] The way that communities respond to emerging technologies drives, in significant part, the development of the law.[101]

However, one notable lack of the otherwise extremely successful virtual worlds literature is the failure to address issues of mobile computing and Mixed Reality.[102] There are several reasons for this. First, virtual worlds have been traditionally defined as graphically rich 3-D persistent spaces in which social groups can gather. But a hidden criterion of virtual worlds is that they be both synchronous[103] (interaction within the world occurs among users who are logged in continuously and at the same time) and persistent[104] (the world exists without the user's presence). Most Mixed Reality applications do not seem at first blush to map to the synchronous or persistent nature of virtual worlds and they use many fewer processor-intensive graphics.

The failure to fully address Mixed Reality leaves a significant gap in the virtual worlds literature. Synchronicity and persistence are, in fact, traits of Mixed Reality experiences, although the "world" that provides the experience in Mixed Reality is the real one. Thus, although the technology itself may not create synchronicity or persistence, Mixed Reality does share these

99. *See* Jankowich, *supra* note 15, at 189 nn.85–86 (discussing open source virtual worlds and the norms generated in them and how this is comparable to the common law process).

100. *See* Joshua A.T. Fairfield, *Castles in the Air: Greg Lastowka's Virtual Justice*, 51 JURIMETRICS J. 89, 90 (2010) ("In so doing, Lastowka frees the field of virtual law from niche status and demonstrates that virtual worlds are participating in the core processes of the common law—they are jurisgenerative spaces. When courts apply law to the new technologies of virtual worlds, they incrementally adapt traditional concepts to a burgeoning technological world. In short, Lastowka demonstrates that virtual law is common law.").

101. *See id.*

102. *See, e.g.*, Barfield, *supra* note 5, at 159–60 (discussing virtually-enriched advertising but failing to address issues surrounding mobile applications of such advertising); Burdon, *supra* note 88, at 8 (discussing GPS and RFID technologies and their use in mobile phones to record a new wealth of geographic information and turning humans into geographical sensors but not delving deeper into mixed reality); King, *supra* note 22, at 125–27 (detailing the growth of mobile advertising but only in the context of RFID chipped mobile phones); *see also* Kang & Cuff, *supra* note 21, at 109 (discussing augmented reality in the context of embedded computing, not mobile computing, and arguing that augmented realities will occur through pervasive computing).

103. *See* Mark W. Bell, *Toward a Definition of "Virtual Worlds,"* 1 VIRTUAL WORLDS RES. 1, 2–3 (2008) (requiring synchronous communication in the definition of a virtual world).

104. *See* Castronova, *supra* note 64, at 5–6.

characteristics of a virtual world. This is unsurprising; a virtual world draws its characteristics from the real one.[105] But what has eluded commentators to date is that virtualized applications, even though they themselves are asynchronous or impermanent, or do not include avatar-based interaction, in fact do form part of a virtual world experience—one that straddles the divide between the virtual and the real.

This Article broadens the virtual worlds literature by examining a new use of virtualization technologies: the augmentation of the real world with rich sets of virtual objects and data. This immeasurably widens the subject matter. Virtual worlds articles are most often about games. Mixed or augmented reality applications can be games, but they are just as commonly shopping, travel, health, or fitness apps. This results in an enormous number of applications. The offerings in the Apple App Store are growing by leaps and bounds and Mixed Reality applications are among the most popular offerings.[106] Services like Foursquare and Yelp, which offer game-like rewards for providing information about locations, goods, and services, have transformed nightlife and fine dining.[107]

Finally, it is possible that Mixed Reality applications may realize certain goals of virtualization technologies before virtual worlds or virtual reality do. For example, although many elements of virtual worlds—including badges, ranks, experience points, and layered fantasy elements—have entered the real world through Mixed Reality, the real world sense of touch has struggled to enter the virtual. Because it is difficult to import touch into virtual worlds, it may be possible to build fantasy worlds on top of real world physicality long before we will import kinetics (i.e., the sensation of touch and balance) into a virtual world. The former is cheap and just beginning to proliferate; the latter is still the stuff of science fiction—imagine the Star Trek holodeck, which provides kinesthetic sensation through force fields. A more practical approach would be to take real objects, such as a blank-faced robot or a moving floor panel (both of which have already been the subject of fascinating demonstrations) and use them as the underlying surface on which to layer augmented reality experiences.[108] So the blank-faced robot becomes

105. *See* Milgram & Kishino, *supra* note 27, at 1324–25; *see also* Boone, *supra* note 53.

106. *See* Shan Li, *Businesses Quickly Adopting Augmented Reality Apps for Consumers*, L.A. TIMES (Oct. 13, 2011), http://lat.ms/GSPDEh (describing the current proliferation of augmented reality apps).

107. *See Yelp for Mobile*, YELP, http://www.yelp.com/yelpmobile (last visited Aug. 4, 2011); FOURSQUARE, https://foursquare.com/ (last visited Feb. 18, 2012).

108. *See* Utsushiomi, *U-Tsu-Shi-O-Mi at Asiagraph 2007*, YOUTUBE (Oct. 16, 2007), http://www.youtube.com/watch?v=htkVlCfCV2M (demonstrating virtual reality overlays on robotic substrates); Joseph L. Flatley, *CirculaFloor Robot Floor Tiles Keep You Moving in*

the kinetic element of a knight or fair maiden; a larger robot provides the kinetic surfaces for a dragon, and in fact whole different landscapes could be layered onto the real one.[109] Or, another example: one company has explored a Mixed Reality "floor" consisting of tiles that constantly move under the user's feet, giving the user the perception that she can keep walking infinitely in any given direction.[110] Mechanical malfunctions of such kinetic interfaces will lead to broken limbs. From the legal perspective, one simple reason to care that kinetics will come sooner to augmented reality than previously thought is that kinetics lead to personal injury lawsuits.

Even today's Mixed Reality applications have implications for physical harm and personal injury suits. By integrating virtuality into the real world, Mixed Reality applications create the threat that people will inevitably ignore some of the real-life aspects of Mixed Reality experiences. Consider the recent unsuccessful case against Google for harm to a pedestrian who followed Google Maps' driving directions and was struck by a car.[111] The information provided was accessible on the Internet and the directions came up in other services as well. The cause was the driver and not the directions themselves. Google did not interact with the end user in a one-to-one manner.[112] Neither realspace nor virtual reality caused the harm.[113] Rather, it was the underlying reality of the car and the road that impacted the pedestrian. While the court rejected the claim in this instance, it is clear that Mixed Reality can have very real legal consequences if users sue for physical harm caused while using these Mixed Reality applications. For this reason alone, a developed legal literature of Mixed Reality will have serious salutary effects for law that is currently in the process of being developed in the courts.

Virtual Reality, ENGADGET (Feb. 26, 2009), http://www.engadget.com/2009/02/26/circula floor-robot-floor-tiles-keep-you-moving-in-virtual-realit/ (demonstrating interactive mobile flooring technology); *see also* Cliff Kuang, *Augmented Reality Floor Simulates Walking on Snow, Pebbles, and Grass*, FAST CO. (Apr. 29, 2010), http://www.fastcompany.com/1633386/aug mented-reality-flooring-simulates-sensation-of-walking-on-snow-pebbles-and-grass; *Moving Floor!*, YOUTUBE (Nov. 6, 2006), http://www.youtube.com/watch?v=DnNWfJveZDI.

109. *See* VERNOR VINGE, RAINBOWS END (2006) (exploring a possible future in which mixed reality would layer 3D virtual experiences on the real world).

110. *See* Flatley, *supra* note 108.

111. *See* Rosenberg v. Harwood, No. 100916536, 2011 WL 3153314 (D. Utah May 27, 2011) (granting Google's motion to dismiss because Google was not negligent).

112. *Id.*

113. *Id.*

2. Pervasive Computing

The fewer than five legal articles that have discussed augmented or Mixed Reality have done so in the context of discussions of pervasive or ubiquitous computing.[114] The literature on law and PerC is limited to a few articles that share a common definition. PerC envisions the virtualization of realspace through the actual embedding of small computer processors placed ubiquitously throughout the environment.[115] Computers would be embedded in walls, floors, ceilings, and toasters. Your refrigerator would automatically update your shopping list, which would be sent to the supermarket for just-in-time delivery to your house. This embedded pervasive computing presence would run constantly and invisibly, providing computing everywhere. Objects would be linked to the network.[116] RFID technology would permit objects to communicate with the rest of the embedded and pervasive computing environment to form the "Internet of things."[117]

But pervasive computing is developing unevenly.[118] Some elements of pervasive computing have advanced rapidly, others not at all, or only slightly.[119] The processors that support mobile phones and the growing

114. *See* Kang & Cuff, *supra* note 21; King, *supra* note 22; *see also* Boone, *supra* note 53, at 104–05 (discussing two traits of pervasive computing: embeddedness and mobility). The first trait has not come to pass but the second characteristic is closer to the mark.

115. *See* E. Casey Lide, *Balancing Benefits and Privacy Concerns of Municipal Broadband Applications*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 467, 472 (" '[T]he Internet of Things,' in which tiny, inexpensive radio transceivers are installed in various everyday items, 'enabling new forms of communication between people and things, and between things themselves.' ").

116. *See* Kang & Cuff, *supra* note 21, at 112 (detailing that PerC is a digital nervous system grafted into the real world space around us, resulting in a networked system).

117. *See* King, *supra* note 22, at 109 n.1 (discussing an International Telecommunications Union report on different technologies, in particular RFID chips, that will lead to an "Internet of things").

118. *See* Justin M. Schmidt, *RFID and Privacy: Living in Perfect Harmony*, 34 RUTGERS COMPUTER & TECH. L.J. 247, 250–52 (2007) (discussing the disparity between active and passive RFID tags: passive tags are small and cheap but have fewer applications while active tags are significantly larger and more expensive and have different uses).

119. *Compare* Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1069–71 (2011) (discussing the use of RFID chips ranging from access cards to buildings, toll payment systems, and passport readers), *with* Adam Powell, *Benchmark Legislation: A Measured Approach in the Fight Against Counterfeit Pharmaceuticals*, 61 HASTINGS L.J. 749, 759–60 (2010) (discussing the use of RFID chips in drugs that are counterfeited and varied benefits such as being written on and the speed of scanning, but also the lack of widespread use due to high and variable costs along with privacy and accuracy concerns), *and* Boone, *supra* note 53, at 10 (identifying ubiquitous computing as "still relatively new and still developing" and the mix of terminology which can include "mobile computing"). Boone's article continues with other terminology that is often included in the ubiquitous computing literature, specifically, "wearable computing, augmented reality" and "near-field communications." *Id.*

stream of user data are in the cloud; they are not present ubiquitously in the local environment.[120] Actual computer processors are more remote than ever, rather than ubiquitous and embedded all around.[121]

On the other hand, the ability to richly augment the real world with data has grown quickly.[122] Information is accessed locally but stored remotely. The phenomenon of hyperlocal data has gone hand-in-hand with the development of remote cloud computing. Thus, there is a non-trivial gap in the pervasive and ubiquitous computing literature: computer processors must not necessarily be located locally in order to provide rich hyperlocal data.[123] Examples are easy to provide: Google Maps augments realspace with significant virtual data and pushes that data out to mobile phones. But the Google Maps data itself is managed and maintained remotely. And this is necessarily so. Massive data sets still require massive amounts of computing power somewhere. The consumer carries the light client program on a mobile device while remote servers perform the heavy computational lifting elsewhere. Pervasive wireless connectivity replaces pervasive computing power.

Conversely, the nanotechnology or micro-microprocessing technology envisioned by pervasive computing has not, largely speaking, come to pass.[124]

---

at 101; *see also* King, *supra* note 22. RFID chips are largely an industry tool for tracking. *See* Schmidt, *supra* note 118. They are present to an extent in mobile computing and in other tools that are consumer driven, for example credit cards, but they act more as a support system for the more widespread and commercially viable mixed reality systems in smartphones. *See* King, *supra* note 22.

120. *See* Kevin Werbach, *The Network Utility*, 60 DUKE L.J. 1761, 1812–13 (2011) ("Most experts participating in a 2010 Pew Foundation Future of the Internet Survey expected that within a decade, remote servers would be the primary means of accessing applications and sharing information, rather than local applications."). Mobile phones also continue to grow and aid in the growth of cloud computing. *Id.* at 1814.

121. *See* Konstantinos K. Stylianou, *An Evolutionary Study of Cloud Computing Services Privacy Terms*, 27 J. MARSHALL J. COMPUTER & INFO. L. 593, 604 (2010) ("Web 2.0 may have made the Internet more interactive, but it is cloud computing that signifies the transition to ubiquitous always-on networking which has the potentials to substitute part of the desktop computer.").

122. *See* Croft, *supra* note 13; Fletcher, *supra* note 13.

123. *See* Werbach, *supra* note 120.

124. *See* Kang & Cuff, *supra* note 21, at 109–12 (presenting the idea of computing in the air, walls, and in our sunglasses, but later identifying the augmentation of experiences with realspace with layers of contextually relevant information). *But see* Jesse Hicks, *DARPA's Next-Gen Wearable Display: Augmented Reality, Holographic Sunglasses*, ENGADGET (Apr. 12, 2011, 11:39 PM), http://www.engadget.com/2011/04/12/darpas-next-gen-wearable-display-augmented-reality-holographi/ (reporting that sunglasses are driven by AR technologies, meaning they are not driven by embedded chips). Kang & Cuff envision "software [that] will manage our datasense and constantly seek out and filter information . . . ." Kang & Cuff, *supra* note 21, at 110; *see also* CHEN, *supra* note 6, at 20, 35 (writing that "[t]he iPhone took Apple's core belief—that software is the key ingredient to hardware's success—and

Computing surrounds us today because it is mobile and moves with users, not because it is ubiquitous, already waiting for users wherever they may go. The difference between mobile and ubiquitous computing carries non-trivial legal implications.

Property law would likely govern a hardware-focused regime like PerC, with the property owner as dominant legal entity.[125] An example would be a PerC-enabled mall, in which RFID chips embedded throughout the mall communicate to the shopper.[126] In contrast, intellectual property and attendant licenses govern software-focused regimes like Mixed Reality,[127] and the application provider or developer maintains control over the servers. The current mobile computing regime is closer to the latter structure. The remote servers that produce Mixed Reality experiences are owned and controlled by the corporate entities[128] that also own the intellectual property rights in the virtual objects or experiences.[129] Use of developers' networks, apps, or programs subjects the users to a license regime that can severely restrict users' rights.[130]

expanded it" and, further, that software is now pervasive). Smartphones are not just one device, but literally hundreds of thousands of things due to apps. CHEN, *supra* note 6, at 9–10. Software is what has become truly pervasive and not computing; instead, computing has become mobile.

125. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1067 (N.D. Cal. 2000) (analyzing an intrusion of hardware under a property regime with the finding that an owner of a computer system has a property right and can exclude others from it); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (finding that an owner of a computer system has a possessory interest and that electronic signals are "sufficiently physically tangible to support a trespass cause of action"); *see also* Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 79–80 (2003) (identifying servers as physical property thereby allowing for a trespass to chattels as the server can functionally be touched).

126. *See generally* Kang & Cuff, *supra* note 21 (discussing the idea of a mall that makes full use of embedded PerC technologies).

127. *See generally* Bradford L. Smith & Susan O Mann, *Innovation and Intellectual Property Protection in the Software industry: An Emerging Role for Patents?*, 71 U. CHI. L. REV. 241 (2004) (finding a strong link between software, its emergence as a vital part of the U.S. economy, and the protections provided by intellectual property laws).

128. *See* John Markoff, *Data Center's Power Use Less Than Was Expected*, N.Y. TIMES (July 31, 2011), http://nyti.ms/wilXuU (identifying that Google not only rents servers but also "generally builds custom computer servers for its data centers").

129. *See Google Terms of Service*, GOOGLE (Apr. 16, 2007), http://www.google.com/accounts/TOS (outlining the relationship between Google and the user with regards to "Google's products, software, services, and websites"). Google is overhauling its terms of service as of March 1, 2012. *Id.*

130. *Id.*; *see also* Vernor v. Autodesk, Inc., 621 F.3d 1102, 1111 (9th Cir. 2010) (outlining how a software vendor can phrase its license agreement to avoid characterization of the transaction as a sale).

In short, the literature on pervasive computing has discussed two distinct topics: the first Mixed Reality,[131] and the second nanotechnology and infrastructure.[132] The literature has focused overwhelmingly on the latter. As such, the current phenomenon of data tagging and hyperlinking realspace (Mixed Reality) remains under-examined. This Article fills this significant gap and provides a legal foundation for a world dominated not by PerC, but by Mixed Reality.

3. Mixed Reality: Patching the Gap

In place of the converging trends predicted by PerC—that both processors and the data processed will become hyperlocal—Mixed Reality is characterized by divergent trends in the location and access of data. As data becomes available hyperlocally, information is increasingly processed and maintained globally. Data is and will progressively be accessed locally from remote and distributed networks. Whether nanotechnology or pervasive computing ever takes off is of secondary importance. Currently, it is clear that a migration to remote computing, with increased reliance on broadband wireless connectivity, is what lies on the computing horizon. Since developers will continue to create tools that permit consumers to use data maintained and processed on the cloud in hyperlocal applications, this Article focuses on the legal significance and implications of this technology virtualizing realspace.[133]

This different approach requires attention to different technologies.[134] Prior discussions of pervasive computing have focused heavily on RFID technology: short-range radio that will permit objects to interact with the

131. *See* Kang & Cuff, *supra* note 21, at 110 ("Preliminary implementations of such augmented reality already exist. For instance, contractors can walk through construction sites with a visor that paints a digital overlay of the approved architectural drawings on the building in progress.").

132. *Id.* at 98–99 n.14 (detailing the use of micromotors, and the reliance on nanotechnology, in addition to varying sizes and forms of devices for pervasive computing). Kang and Cuff detail the infrastructure of pervasive computing under the idea of embeddedness, where computers are embedded everywhere and are capable of wireless communications. *Id.* at 97.

133. *See also* Jamais Cascio, *Filtering Reality, How an Emerging Technology Could Threaten Civility*, ATLANTIC MAG. (Nov. 2009), http://www.theatlantic.com/magazine/archive/2009/11/filtering-reality/7713/ (detailing augmented reality and current apps, such as Layar, that allow users to "see location-specific data superimposed over their surroundings" in addition to upcoming technologies planned by Sony, for example wearable AR devices like sunglasses).

134. *See* CHEN, *supra* note 6, at 194–99 (detailing different AR technologies, such as smartphones, headwear, eyewear, and sensory specific options that go beyond just visual, such as audio cues from earpieces).

environment. RFID will play a role, as it currently does, but only in a support role for Mixed Reality apps.[135] The relevant technology is the expanding reach of mobile telecommunications broadband networks—Evolution Data Optimized ("EVDO" or "3G") and Long-Term Evolution ("LTE" or "4G")—that deliver broadband technology to smartphones and tablets.[136]

This Article also fills an important gap in the virtual worlds literature. The virtual worlds literature has not addressed Mixed Reality technologies. This is a significant oversight given that browser and mobile delivery are the fastest growing methods of delivery of virtual experiences. Further, the virtual worlds literature has been characterized by a willingness to treat virtual worlds as a separate reality governed by distinct rules separate from realspace (i.e., the rules of intellectual property).[137] Mixed Reality necessarily puts an end to that distinction. Virtual worlds cannot be regulated independently from realspace when virtual objects and places increasingly are a part of realspace itself.

In the Part that follows, this Article grapples with some of the problems that Mixed Reality applications raise for law, both broadly and as a matter of specific challenges that will arise within individual legal contexts. In so doing, this Article highlights that the law that governs virtual worlds—mostly intellectual property and licensing law—increasingly supplants or subverts the legal regimes that traditionally govern everyday life.[138] What we once owned, we will in the future only license.[139] What was once a simple breach

135. *See* King, *supra* note 22.

136. *See* Jeffrey Paul Jarosch, *Reassessing Tying Arrangements at the End of AT&T's iPhone Exclusivity*, 2011 COLUM. BUS. L. REV. 297, 330–31 (detailing the growth in wireless networks from 2000 to 2009).

137. *See, e.g.*, Jack M. Balkin, *Law and Liberty in Virtual Worlds*, *in* STATE OF PLAY: LAW, GAMES, AND VIRTUAL WORLDS 86, 94 (Jack M. Balkin & Beth Simone Noveck eds., 2006) (arguing that real world laws and legal bodies should allow virtual worlds to construct their own standards for internal needs); Edward Castronova, *The Right To Play*, 49 N.Y.L. SCH. L. REV. 185, 204 (2005) (arguing for a law of iteration where, for example, virtual economies would be governed by a body of law that was completely separate from real world economies).

138. *See* Vernor v. Autodesk, Inc., 621 F.3d 1102, 1111–12 (9th Cir. 2010) (finding that the software owner was not the owner and therefore could not sell it to other users); *see also* Bowers v. Baystate Techs., Inc., 320 F.3d 1317, 1325–26 (Fed. Cir. 2003) (detailing that private parties are able to contract out of the limited ability to reverse engineer software, a fair use under the exemptions of the Copyright Act); Davidson & Associates, Inc. v. Internet Gateway, Inc., 334 F. Supp. 2d 1164, 1181 (E.D. Mo. 2004), *aff'd sub nom.* Davidson & Associates v. Jung, 422 F.3d 630 (8th Cir. 2005) ("The defendants in this case waived their 'fair use' right to reverse engineer by agreeing to the licensing agreement.").

139. *See Vernor*, 621 F.3d at 1111; *see also* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459 (2006) (finding that contracts, such as license agreements, "clickwrap" and

of contract may now be a hacking crime or potential copyright infringement.[140] The following Sections chronicle the replacement of legal systems designed to secure citizens' reputational, property, and privacy interests with intellectual property licenses that endanger all of these interests.[141]

III. THE LAW OF MIXED REALITY

The technological revolution of Mixed Reality is well underway. Reality is being hyperlinked, data tagged, indexed, and made searchable in the same way that the bulk of human knowledge was made accessible suddenly and surprisingly through the hyperlinked Internet. The coming legal revolution in response to Mixed Reality will both resolve existing legal debates and raise new, and potentially troubling, questions. For example, a developed theory of Mixed Reality finally puts an end to the enduring and erroneous theoretical idea of the Magic Circle, a metaphorical legal boundary that commentators have supposed separates the real world from virtual ones.[142] Virtual worlds cannot be deemed legally separate from the real one.[143] All virtual worlds are to some extent mixed: they are experienced by real world people, who interject elements of reality into the virtual world.[144] The world may be virtual, but the economic, artistic, and even romantic lives of the participants are quite real.[145]

"browsewrap", and Terms of Use, have grown in popularity and, critically, are increasingly enforced by courts).

140. *See* MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 939 (9th Cir. 2010) (setting out the contractual terms that limit the scope of a license as a "condition" and all other license terms as "covenants"). A user can still violate a covenant and thereby breach a contractual term. If a user were to violate a condition of a license agreement, copyright would be implicated. *See also* Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.). The DMCA contains three provisions that create a framework to address circumvention of technological measures that protect copyrighted works. *See* 17 U.S.C. § 1201(a)(1)–(2), (b)(1) (2006); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996) (describing that UCC § 2-204(1) provides for different formations of contracts, such as a prompt on a computer screen, which can prevent access). ProCD proposed a contract that a buyer would accept by *using* the software after having an opportunity to read the license at leisure.

141. *See MDY*, 629 F.3d at 938 (detailing a particular Term of Use and the prohibition of cheats, hacks, or other third party software, essentially requiring fair play).

142. *See* Castronova, *supra* note 137, at 200–05.

143. *See* Fairfield, *supra* note 74.

144. *Id.* at 825.

145. *See* Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593 (E.D. Pa. 2007) ("While the property and the world where it is found are 'virtual,' the dispute is real.").

Although the Magic Circle is now broken, the legal effects of the Mixed Reality revolution are uncertain. Laws that govern the real world will apply to both elements of the Mixed Reality experience: intellectual property and e-commercial contracts will continue to govern the software and firmware in the devices; real-world property and tort law will continue to govern where users can go and what they can do in the real world. However, the principal issue between these two spheres is the encroachment of IP and e-commercial contracts into realspace via the virtualization of realspace. Will intellectual property law come to govern the extent to which consumers can use their own real and chattel property,[146] just as it now governs what applications consumers may use on their own devices? Without a developed theory of Mixed Reality, IP and e-commercial contracts will overtake property and torts in realspace.

To supplement these basic conclusions about the current trajectory of the law, the following Sections analyze the biggest areas of shift by category: contract law, tort law, property law, and privacy law. There are of course other important legal shifts that this Article must necessarily leave out, if only for space reasons. An example would be free speech: a shift will occur here too, when most of human discourse switches from telephone or email to corporate-controlled social networks, like Twitter, Google+, or Facebook.[147] However, the Article presents selected examples that highlight a pattern in the legal shift: an accelerating trend away from private property and consumer choice in a free market,[148] and toward corporate hegemonic

146. *See* Bowers v. Baystate Techs., Inc., 320 F.3d 1317, 1323–34 (Fed. Cir. 2003) (evaluating the issues using copyright and patent law); Davidson & Associates, Inc. v. Internet Gateway, Inc., 334 F. Supp. 2d 1164, 1187 (E.D. Mo. 2004), *aff'd sub nom.* Davidson & Associates v. Jung, 422 F.3d 630 (8th Cir. 2005) (finding in favor of licensor); *see also MDY*, 629 F.3d at 938–43 (framing the claim of improper use of software in copyright); Lemley, *supra* note 139, at 460 (placing shrinkwrap, clickwrap, and browsewrap licenses under the umbrella "terms of use" because they all seek to control the extent to which buyers of software, or visitors to a site, can use that software or site).

147. *See* Miguel Helft, *Facebook Wrestles with Free Speech and Civility*, N.Y. TIMES (Dec. 12, 2010), http://www.nytimes.com/2010/12/13/technology/13facebook.html (" 'Facebook has more power in determining who can speak and who can be heard around the globe than any Supreme Court justice, any king or any president,' said Jeffrey Rosen, a law professor at George Washington University who has written about free speech on the Internet. 'It is important that Facebook is exercising its power carefully and protecting more speech rather than less.' "); Ashlee Vance & Miguel Helft, *Hackers Give Web Companies a Test of Free Speech*, N.Y. TIMES (Dec. 8, 2010), http://www.nytimes.com/2010/12/09/technology/09net.html (detailing the tension between the high praise received by Twitter and Facebook as outlets of free speech and their corporate aspirations of both because both rely so heavily on advertising).

148. *See* CHEN, *supra* note 6, at 92 (discussing the negative feedback to Apple's App Store and its legal agreements with developers). "[I]f a person makes an app for the iPhone,

control over consumers,[149] exercised by the threat of intellectual property lawsuits based on mass-market consumer application End User License Agreements ("EULAs") or website Terms of Use ("TOUs").[150]

A. CONTRACT LAW: EULAS AND INTELLECTUAL PROPERTY LICENSING WILL GOVERN EVERYDAY LIFE

Mixed Reality technologies on mobile computing devices augment our daily lives with rich data. But these technologies also bring the dangerously flawed law of copyright to the real world. The laws governing the licensing of intellectual property were intended to govern intangibles, not the tangible world.[151] The basic economic assumption underlying intellectual property law is that expression is costly to produce and cheap to copy.[152] This is the foundation of the copyright system.[153] Since expressions are so cheap to copy, fewer people would invest time and money in creation. And indeed,

he has to make it Apple's way or it won't be offered in the App Store. He has to play by Apple's strict rules." *Id.* "Apple must approve every iPhone app before it goes up for sale in the App Store, and this means that the corporation can regulate and censor content however it wishes." *Id.*; *see also* Lemley, *supra* note 139, at 470–72 ("The problem is that the shift from property law to contract law takes the job of defining the Web site owner's rights out of the hands of the law and into the hands of the site owner.").

149. *See* Brian X. Chen, *Programmer Raises Concerns About Phone-Monitoring Software*, N.Y. TIMES BITS (Dec. 1, 2011 4:58 PM), http://bits.blogs.nytimes.com/2011/12/01/programmer-raises-concerns-about-phone-monitoring-software/ (discussing the newly discovered data-collection software, Carrier IQ, that major cellular phone carriers have installed and that collects data such as users' locations and telephone activity).

150. *See* Lemley, *supra* note 139, at 470–72; *see also MDY*, 629 F.3d at 938–39 (discussing the ability of a company to write a contract such that the buyer owns or licenses the software and further that restrictions can be placed within such a license agreement that would allow a company to later sue for violations of that agreement based on a breach of its terms resulting in a contract breach or even copyright infringement); Lemley, *supra* note 139, at 466–68 (discussing the rise in enforcement of license agreements and TOSs by courts).

151. Michael Grynberg, *The Judicial Role in Trademark Law*, 52 B.C. L. REV. 1283, 1335 (2011) ("Intellectual property gives functional property rights to the creators of intangible goods.").

152. *See* Gideon Parchomovsky & Peter Siegelman, *Towards an Integrated Theory of Intellectual Property,* 88 VA. L. REV. 1455, 1466–67 (2002) (stating that absent legal protections, competitors would be able to copy expressive works and inventions without incurring the initial costs of production which, in turn, would drive down the market price leaving original authors and inventors without the ability to recover their initial production costs).

153. *See* Smith & Mann, *supra* note 127, at 241–42 (discussing the role of IP protection in incentivizing developers to invest in their programming as it prevents copying by protecting the original expression and aids in preventing copies that diminish the return on development costs).

many of the early internet fights were about copying.[154] The Recording Industry Association of America ("RIAA") famously sued teens and grandmothers across the nation for copying MP3 files.[155]

Copying—the driving concern of copyright law—turned out to be a bad paradigm for internet technologies. Internet technologies incentivize users to stream content rather than copy content because it is more expensive to maintain a local copy of a file on your own computer than it is to stream it.[156] As a result, the copyright system does little to inform the circumstances surrounding internet technologies. Copyright also serves as a bad paradigm because copyright holders wanted to do far more than restrict their customers from rote copying of copyrighted materials—they wanted control over their customers.[157] Beyond the right to control copying, copyright holders often asserted the ability to prevent customers from doing business with the copyright holder's competitors.[158]

Unfortunately, copyright law has indulged copyright holders in this regard.[159] Early case law in the Ninth Circuit (a critical circuit for online

154. *See, e.g.*, Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1231 (D.C. Cir. 2003); Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072 (9th Cir. 1999).

155. *See* John Schwartz, *Record Industry May Not Subpoena Online Providers*, N.Y. TIMES (Dec. 19, 2003), http://nyti.ms/GSNpVq.

156. *See* Kier Thomas, *Cloud Computing: The Executive Summary*, PC WORLD (Dec. 29, 2010), http://www.pcworld.com/businesscenter/article/215134/cloud_computing_the_executive_summary.html (noting that cloud computing is cheaper than maintaining local files for businesses).

157. *See* Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1201 (Fed. Cir. 2004) (discussing The Chamberlain Group's arguments as seeking to control consumers options); Walter S. Mossberg, *Media Companies Go Too Far in Curbing Consumers' Activities*, WALL ST. J., Oct. 20, 2005, at B1, *available at* http://on.wsj.com/yiv0Sv (explaining that DRM comes in several forms, is widely used, and controls not just whether something can be copied, but also whether it can even be accessed, such as with TiVo and a given TV program expiring after a certain period of time).

158. Aaron Perzanowski & Jason Schultz, *Digital Exhaustion*, 58 UCLA L. REV. 889, 901 (2011) ("Today, device makers and content distributors can easily introduce barriers to compatibility . . . . [S]hifting legal and technological landscapes, marked by the introduction of digital works and technological measures designed to restrict lawful access, have created serious concerns over lock-in."); *see also Chamberlain*, 381 F.3d at 1201 (finding that the copyright holder, Chamberlain, sought "to leverage its sales into aftermarket monopolies—a practice that both the antitrust laws . . . and the doctrine of copyright misuse . . . normally prohibit"); CHEN, *supra* note 6, at 6 (discussing the emerging use of app stores by TV makers and car companies such as Ford, "all with the common goal of trapping consumers inside their product lines").

159. *See, e.g.*, Phillip A. Harris Jr., *Mod Chips and Homebrew: A Recipe for Their Continued Use in the Wake of* Sony v. Divineo, 9 N.C. J.L. & TECH. 113, 134 (2007) ("Prior to the DMCA, courts took a very liberal view on reverse engineering of video game protections and allowed

technologies) held that copyright could be used to control behavior in an entirely new set of cases to which it had been previously inapplicable.[160] According to these cases, merely loading a computer program for a purpose outside of the software license agreement may constitute copyright infringement.[161] Thus, while flipping through a book at a bookstore never implicated copyright law (because no copy was being made), accessing the same material on a Kindle or iPad does implicate copyright law due to the Ninth Circuit's reading of the copyright statute.[162]

it for 'intermediate copying.' After the creation and implementation of the DMCA, however, courts showed a stricter approach to copying and held that the interest in protecting copyright holders' security measures is greater than the interest of fair users that may attempt to use the functional components of intellectual property to create new platforms and software." (citation omitted)); Joseph E. Van Tassel, *Remote Deletion Technology, License Agreements, and the Distribution of Copyrighted Works*, 97 VA. L. REV. 1223, 1236 (2011) ("Furthermore, [the] balance of intellectual property rights arguably already skews in favor of the copyright holder, so courts should be wary of further curtailment of users' rights through the use of license agreements.").

160. *See* Wall Data, Inc. v. Los Angeles Cnty. Sheriff's Dep't, 447 F.3d 769 (9th Cir. 2006) (finding that because defendant was a licensee and not an owner, it therefore infringed the plaintiff's copyright by copying the software and installing it on multiple computers in violation of the license agreement); Triad Sys. Corp. v. Se. Express Co., 64 F.3d 1330 (9th Cir. 1995); MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 519 (9th Cir. 1993) (creating the random access memory ("RAM") copy doctrine: "[S]ince we find that the copy created in the RAM can be 'perceived, reproduced, or otherwise communicated,' we hold that the loading of software into the RAM creates a copy under the Copyright Act.").

161. The RAM copy doctrine makes it a copyright violation to violate any term of a license agreement where the software is copied into the computer's RAM. *See* MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 941 (9th Cir. 2010) ("The rationale would be that because the conduct occurs while the player's computer is copying the software code into RAM in order for it to run, the violation is copyright infringement.").

162. *See MAI*, 991 F.2d at 519–20; *MDY*, 629 F.3d at 941. *But see* Cartoon Network LP v. CSC Holding, Inc., 536 F.3d 121 (2d Cir. 2008) (finding that an embodiment and a durational requirement needed to be met in order for a data stream to be "fixed"). *MAI* did not require a durational requirement, only an embodiment. *See MAI*, 991 F.2d at 519–20 (finding temporary storage on RAM to constitute a copyright violation). Circuits have varied in their adoption of the *MAI* holding, and the Second Circuit's decision presented a circuit split concerning, for example, whether streaming data results in a momentary copy. This apparent split caused the parties to *Cartoon Network* to seek further review. *See* KATE M. MANUEL, CONG. RESEARCH SERV., RL34719, CARTOON NETWORK LP V. CSC HOLDINGS, INC.: REMOTE-STORAGE DIGITAL VIDEO RECORDERS AND COPYRIGHT LAW 10 n.90 (2009), *available at* http://ipmall.info/hosted_resources/crs/RL34719_090706.pdf (noting that in June 2009 the Supreme Court denied certiorari for review of the apparent circuit split created by the Second Circuit's ruling). The Supreme Court's denial of certiorari suggests that the circuit split is not significant enough to justify review. The circuit split has not affected the large bulk of client-server architecture applications, in which there is undoubtedly a copy of the creator's content made on the local client.

Shifting a simple breach of contract claim into a claim for intellectual property infringement has several immediate effects. Breach of contract generally generates expectation damages. Copyright infringement, however, entails a statutory remedy system as detailed in 17 U.S.C. § 504(c).[163] This statutory regime is the mechanism through which the RIAA can seek millions of dollars in damages from teenagers.[164] Each download of a separate registered work constitutes a separate infraction.[165] This shift alone significantly increases corporate control over consumer behavior. And the shift from the traditional remedy of expectation damages to statutory damages also changes consumers' incentives to breach abusive and overreaching online contracts. Where the company's expectation damages from a consumer's breach of an EULA are vanishingly small, the statutory damages regime of copyright can turn litigation against one's own customers from a losing strategy to a profit center.[166]

The shift away from consumer rights and toward corporate control over consumers' daily lives via EULAs and TOUs is one of the largest unheralded shifts in law of our generation. Threats of copyright infringement suits[167] require consumers to comply with a wide range of restrictions utterly

163. *See* 17 U.S.C. § 504(c) (2010) (creating a framework of awards for infringements of one particular work, instead of multiple copies of one work, no less than $750 and no more than $30,000 based on the court's determination). Where the infringement was committed willfully, and the copyright owner sustains the burden of proving as such, the damage award jumps to no more than $150,000 but where the infringer is able to demonstrate they were not aware and had no reason to believe they were infringing a copyright, the damage is reduced to no less than $200 at the court's discretion. *Id.*

164. *See* Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. 439, 441 nn.4–5 (2009) ("Although Congress intended this designation to apply only in 'exceptional cases,' courts have interpreted willfulness so broadly that those who merely should have known their conduct was infringing are often treated as willful infringers."). There have been several cases in which courts awarded amounts as large as $80,000 per infringed song and a final award as large as $1.92 million, even where the actual damages determined were near $50. *Id.* at 442–43 nn.13–14.

165. *See* § 504(c) (providing for an award of "statutory damages for all infringements involved in the action, with respect to any one work").

166. *See id.* (outlining statutory damages for copyright infringement).

167. *See* Viva R. Moffat, *Super-Copyright: Contracts, Preemption, and the Structure of Copyright Policymaking*, 41 U.C. DAVIS L. REV. 45, 64 (2007) ("Although these terms may rarely be enforced, at least for now, their consistent inclusion and their consistent, but not uniform, language indicates that the lawyers or website developers who are including these terms seek to reserve their rights to bring breach of contract actions (or to send cease-and-desist letters), possibly coupled with copyright infringement claims seeking copyright's statutory damages.").

unrelated to the making of copies.[168] Facebook provides one example of how copyright law significantly shifts the balance of power to producers from consumers of internet technology. Facebook asserts a perpetual license in all of its users' private information.[169] Facebook also ferociously limits what users can say. For example, a recent academic conference focusing on the use of internet kill switches in stifling speech was itself ironically stifled when it tried to advertise via a Facebook page because Facebook does not permit use of the term "Internet kill switch."[170] One might not be bothered by such decisions were it not that Facebook surpasses email as the means preferred for communication by many Americans.[171] Threats of copyright liability—like the threat by Facebook—attach any time someone purchases software, visits a website, or uses a social media site.

As intrusive as copyright licensing is for purely online computing, it is far more so for the next generation of internet technologies—Mixed Reality and mobile computing. Now, there exists the danger that the copyright law dominating online interactions will flow into Mixed Reality and govern its users in realspace. This new breed of online contracts impacts legal regimes across the board because our current system of law permits parties to alter almost any background legal arrangement via consent.[172] To enter a digital store a consumer must agree to the store's terms.[173] By remaining on a website, a consumer ostensibly signs a contract. Engaging in online

168. *See, e.g.*, MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 938 (9th Cir. 2010) (requiring users to use software only in the ways allowed by the agreement).

169. *See Statement of Rights and Responsibilities*, FACEBOOK, § 2(1), http://www.facebook.com/terms.php (last updated Apr. 26, 2011) ("[Y]ou specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.").

170. *See CLIP Roundtable: Internet Switch—National Security or Public Repression?*, FACEBOOK (Feb. 10, 2011), http://www.facebook.com/event.php?eid=194151337269200 (missing the "kill" in the title after being edited).

171. *See* Matt Richtel, *Email Gets an Instant Makeover*, N.Y. TIMES (Dec. 20, 2010), http://www.nytimes.com/2010/12/21/technology/21email.html (noting how many people in the younger generations prefer other communications media, such as Facebook, to email).

172. *See* Davidson & Associates, Inc. v. Internet Gateway, Inc., 334 F. Supp. 2d 1164, 1184 (E.D. Mo. 2004), *aff'd sub nom.* Davidson & Associates v. Jung, 422 F.3d 630 (8th Cir. 2005) (finding consent to the software agreement); *see also* Fairfield, *supra* note 74, at 831–35 (noting how games allow individuals to alter even the rules of society with regards to one another through consent).

173. One of the most notable examples of this is the iTunes splash screen, displaying the iTunes terms of service. *See Terms and Conditions*, APPLE, http://www.apple.com/legal/itunes/us/terms.html#SALE (last updated Oct. 12, 2011).

transactions also requires a consumer to agree to the contractual terms and conditions of the site.

For example, on smartphones Google Maps is an indispensable application that permits use of the telephone as a GPS device. But Google Maps, like other Mixed Reality apps, also utilizes GPS technology to track,[174] collect, package, and resell the real world physical location of smartphone users to a broad array of third parties.[175] To use Google Maps, consumers must consent to Google's terms, which also effectuates consent to the tracking process just mentioned.[176] Under the current legal regime, these tracking activities are protected under the law governing online contracts (EULAs and TOUs) because users have given their consent in order to use the services. But this is a poor legal framework for Mixed Reality because it fails to recognize the "reality" aspect of Mixed Reality and, most importantly, how Mixed Reality applications are coming to affect the real world.

A comparison may clarify: consider the different reactions that Google's surveillance of its customers received online and offline. Online, Google retains all of its users' searches, ties them to specific user profiles, and further ties all users' online browsing habits (whether tracked by Google cookies on the company's own sites, or tracked through the Google advertising service on third-party sites, or some combination of the two).[177] While the practice is

174. There are multiple layers of tracking. Even if app providers did not collect real-world location information, telephone companies themselves record the browsing habits and IP addresses assigned to their smartphone customers, as well as cell-site location information, which is the information on where the telephone user has traveled in real life as indicated by the cell towers that the mobile phone contacts. And even if mobile phone companies did not record this information, internet advertising giants leverage their vast consumer information databases to track wherever their customers browse online, all without anything more than the figleaf of consent of a buried clause in an electronic contract that no consumer ever sees or reads. (And what would consumers do if they did read it and objected? Use the Internet without Google?) The confluence of these technologies means that all of a user's activity—online and off—is tracked and recorded.

175. *See* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, WALL ST. J. (Apr. 22, 2011), http://on.wsj.com/zp2Euo ("Google and Apple are gathering location information as part of their race to build massive databases capable of pinpointing people's locations via their cellphones. These databases could help them tap the $2.9 billion market for location-based services—expected to rise to $8.3 billion in 2014."). "[S]ome of the most popular smartphone apps use location data and other personal information even more aggressively than this—in some cases sharing it with third-party companies without the user's consent or knowledge." *Id.*

176. *See Privacy Center—Privacy Policy*, GOOGLE, http://www.google.com/intl/en/privacy/privacy-policy.html (last modified Oct. 20, 2011) (outlining Google's use of personal information, which includes using location data to "improve" its services for users).

177. *See* Anne Klinefelter, *When To Research Is To Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 VA. J.L. & TECH. 1, 6–9 (2011) (detailing how web

met with some criticism, it is generally accepted that users of their services consent to these practices. But a similar practice of data collection, when injected into the real world, got Google into serious legal trouble. Google Streetview cars accessed individuals' open home wireless networks as the cars roamed around taking pictures for Google Maps, collecting data from those networks.[178] Even though the result was basically the same—collection of user data—the fact that the activity took place in a tangible way made a significant difference in the way the practice was perceived. As a result, lawsuits were filed across the United States, and state attorneys general began to investigate the search giant for possible illegal wiretapping and invasions of communication privacy.[179] The real difference in this comparison is not between "online" and "offline" collection of data—after all, the Streetview cars tapped into wifi connections—but whether there was the barest figleaf of contractual consent in place. Google ostensibly secures consent for an enormous amount of intrusive surveillance on its customers as soon as users surf to its web page.[180] Streetview cars did not have any such contractual figleaf.

The fighting question for Mixed Reality applications will be whether such online contracts of adhesion will finally be pushed down into the real world, such that courts will protect intrusions—like those of the Streetview car—under the theory that consumers have consented to the surveillance.[181] Google already engages in online surveillance operations gathering data far more comprehensive than any of the data gathered by Streetview, but it is privileged to do so under a strained reading of contract law.[182]

---

browsing, searching, and online activities in general—including the use of Google—give rise to attorney-client confidentiality concerns due to the data being saved and indexed).

178. *See* Elec. Privacy Info. Ctr. (EPIC), *Investigations of Google Street View*, EPIC.ORG, http://epic.org/privacy/streetview/ (last visited Oct. 31, 2011) (summarizing the various investigations around the world into Google's practice of collecting data from unencrypted wireless networks).

179. *Id.*

180. *See Google Terms of Service*, *supra* note 129.

181. *See* Elinor Mills, *Carrier IQ Faces Lawsuits, Lawmaker Seeks FTC Probe*, CNET (Dec. 2, 2011, 1:09 PM), http://cnet.co/xgWjcX (describing the lawsuit filed against Carrier IQ as performing surveillance without consumer consent). Carrier IQ responded to the criticisms by claiming that it was assisting carriers in gathering data, and at least one carrier stated that its practices of using Carrier IQ did not violate its privacy policy. David Sarno & Tiffany Hsu, *Carrier IQ Defends Itself in Furor over Smartphone Users' Privacy*, L.A. TIMES (Dec. 2, 2011), http://lat.ms/GSNVmp. At the time of this writing, Carrier IQ has not issued a formal response to the suits.

182. *See* Lemley, *supra* note 139, at 468–70 (citing *ProCD*'s questionable legal reasoning based on incomplete reliance upon the UCC, in particular §§ 2-204, -207, and -209, with the subsequent legal reality that these rigid contracts are typically upheld in favor of their corporate authors).

We have come full circle. The special set of rules that were originally intended to govern intangible, intellectual property now govern the everyday, walkabout lives of U.S. citizens. American citizens do not functionally own their private information and cannot stop the indiscriminate recording of data about their everyday lives short of refusing to use cell phones and the Internet. What is needed is a robust path forward based on existing, established contract, tort, property, and privacy law. A legal regime not muddled by a strained reading of intellectual property law will protect consumers, scale back untrammeled corporate control of consumer information, and return copyright to its original role of protecting copying of creativity, rather than controlling the economic and intimate lives of citizens. The following Sections explore the issues in other areas of law, before offering proposals for re-balancing the law in Part IV.

B. TORT LAW: CYBERDEFAMATION AND MIXED REALITY REPUTATION SYSTEMS

The Mixed Reality future will include facial recognition software that is able to access reputational ratings of people the user runs across in her everyday life.[183] Tagging real people with data raises obvious issues relating to the law of reputational interests, which acts to protect individuals against the publication of false statements made against their image.[184] Where employers now Google applicants, in the future they will merely check the person's online reputation with a range of online reputation providers and social networks. Once personally-tagged reputation and personal information becomes ubiquitously available to everyone with a smartphone, the temptation to manipulate or poison that information to cause reputational harms will inevitably arise.

Such reputational harms can already be found in the purely online context.[185] For example, an early Google bomb—using search engine

183. *See* John Biggs, *iOS 5 To Have Powerful Face Detection*, TECHCRUNCH (July 27, 2011), http://techcrunch.com/2011/07/27/ios-5-to-have-powerful-face-detection/ (reporting on Apple's purchase of a facial recognition software company, Polar Rose, and the plan to incorporate it into Apple's iPhone operating system); Ben Parr, *Top 6 Augmented Reality Mobile Apps*, MASHABLE (Aug. 19, 2009), http://mashable.com/2009/08/19/augmented-reality-apps/ (describing a mobile app called Augmented ID that recognizes a person's face and pulls up information about that person).

184. *See* RESTATEMENT (SECOND) OF TORTS § 569 (1977) ("One who falsely publishes matter defamatory of another in such a manner as to make the publication a libel is subject to liability to the other although no special harm results from the publication.").

185. Kai Ma, *Dan Savage Threatens To 'Google Bomb' Rick Santorum, Yet Again*, TIME NEWSFEED (July 28, 2011), http://newsfeed.time.com/2011/07/28/dan-savage-threatens-to-google-bomb-rick-santorum-yet-again/.

optimization to prioritize the results of the "bomber" on Google—targeted Senator Rick Santorum.[186] Political detractors of the senator created an off-color definition of the senator's name and then raised the search rank of the alternative result by crosslinking and referencing the neologism.[187] The end result was that searches on Google for the senator's name would find the alternative definition in the first page of results.[188]

Because the Internet has become the primary purveyor of both personal and professional reputational information, the risk of harm is magnified. Employers Google prospective applicants.[189] Social networks like LinkedIn manage professional connections.[190] eBay maintains reputation systems for third party vendors, facilitating transactions between parties that otherwise would not trust one another.[191]

Under the current legal and statutory regime, however, companies that create and maintain reputational networks lack incentive to keep reputational data accurate. This is because § 230 of the Communications Decency Act ("CDA")[192] generally immunizes interactive computing services providers from tort lawsuits stemming from inaccurate data supplied by users of the service.[193] Defamation law governs reputational harm offline—where there is no corresponding immunity for providers of reputational information. Thus,

186. Tom McNichol, *Your Message Here*, N.Y. TIMES (Jan. 22, 2004), http://www.nytimes.com/2004/01/22/technology/your-message-here.html (explaining the phenomenon of "google bombing").

187. *See* Marziah Karch, *Google Bombs Explained*, ABOUT.COM, http://google.about.com/od/socialtoolsfromgoogle/a/googlebombatcl.htm (last visited Dec. 12, 2011) (noting that Santorum's name was linked to the definition of a lewd phrase through a Google bomb).

188. *See id.*

189. *See Employers Google Applicants*, ABC NEWS (Apr. 28, 2007), http://abcnews.go.com/Business/video?id=3083837.

190. *See What Is LinkedIn?*, LINKEDIN, http://www.linkedin.com/static?key=what_is_linkedin&trk=hb_what (last visited Oct. 31, 2011) (describing the professional networking qualities of LinkedIn).

191. *See Detailed Seller Ratings*, EBAY, http://pages.ebay.com/help/feedback/detailed-seller-ratings.html (last visited Oct. 31, 2011) (describing eBay's seller rating system and how it is used to determine seller quality).

192. 47 U.S.C. § 230 (2010).

193. *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009); Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008); Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008); Chi. Lawyers' Comm. for Civil Rights v. Craigslist, 519 F.3d 666 (7th Cir. 2008); Mazur v. eBay, No. C 07-03967 MHP, 2008 WL 618988, at *1 (N.D. Cal. Mar. 3, 2008); Doe v. SexSearch.com, 502 F. Supp. 2d 719 (N.D. Ohio 2007) (dismissing claim against online site SexSearch on grounds that plaintiff's claim based on SexSearch's promise that all users were over 18 was barred by CDA § 230 when a minor entered false data as to age), *aff'd*, 551 F.3d 412 (6th Cir. 2008) (affirming on grounds of failure to state a claim, but declining to adopt district court's reading of CDA § 230).

online service providers generally avoid liability where offline providers incur liability. This duality makes the existence and proliferation of false or misleading reputational information that much more appealing on the Internet. This Section will explore these problems with online reputation in turn.

An example may help to clarify the current state of the law and the problems Mixed Reality raises. Imagine an online dating website that assures users that its users are unmarried and have not committed a felony. User A lies about her marriage status and criminal record. User B dates user A, and is harmed as a result. Let us also assume that the site knowingly or willfully failed to implement measures that would easily have detected A's falsehoods. On these facts, the caselaw as to the website's liability is split.[194] Section 230 clearly seems to bar any lawsuit based on the false information that user A entered.[195] However, courts are split over whether the site can be held liable for its failure to live up to promises regarding the data added by users.[196] Some courts seem to lean toward immunity: since the inaccuracy in the site's representation was caused by the third party's false data entry, the site would be immune to any lawsuits for failing to remove false data.[197] Other interpretive approaches might lean in the opposite direction, reasoning that the claim that the dates were "safe" was itself a representation by the company, not a representation by a third party user of the site.[198]

This system of online content management leads to very strange incentives. The corporate curator of a reputation network has immunity from

194. Joshua Dubnow, *Ensuring Innovation as the Internet Matures: Competing Interpretations of the Intellectual Property Exception to the Communications Decency Act Immunity*, 9 NW. J. TECH. & INTELL. PROP. 297, 307 (2010) ("While the courts have reached two competing interpretations of § 230(c)(1) and (e)(2) of the Communications Decency Act, this split must ultimately be resolved because of the vastly different outcomes to which each interpretation leads.").

195. *See* § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

196. *See Barnes*, 570 F.3d at 1109 (denying Yahoo! § 230 liability where a Yahoo! associate made a direct promise to remove nude pictures of plaintiff posted by a third party); *Fair Hous. Council*, 521 F.3d at 1176–77 (denying Roommates.com § 230 immunity where it exercised such control over the statements of the users that it functionally became the source of their illegal housing advertisements); *Mazur*, 2008 WL 618988, at *14 (denying eBay § 230 immunity where eBay itself made representations about the nature of certain auctions).

197. *See SexSearch.com*, 502 F. Supp. 2d at 727–28.

198. *See* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 397, 411, 479 (2010) (explaining that the first empirical study of § 230 reveals that the statute has been haphazardly applied by courts and has led to mixed—but generally positive—outcomes for providers).

suit based on third party false representations of trustworthiness,[199] but also directly profits from a high overall reputation average within the network. For example, new apps in the Android app market appear to receive a five-star rating at the outset.[200] This rating is then modified by third party reviews of the software. The overall sense that this generates is that Android apps are high quality and safe, when the reality is that many are merely new. In fact, due to Android's popularity, dangerous and fraudulent apps are at an all-time high[201] and benefit disproportionately from the appearance of trustworthiness that the Android market creates. Legal precedent appears to incentivize the network to make untrue statements about the high level of trustworthiness of the network. This exacerbates the tension between the network's financial stake in a good reputation and the very point of such a network (to help users detect bad actors). Even if a bad actor's false inputs into the reputation network render the reputation provider's statements untrue, there is a high likelihood that network provider will be immune from liability.[202]

This leads back to the problem of online licensing and increasing control over consumers. At the same time that copyright law has given online service providers unprecedented power over consumers, courts have also granted providers unprecedented immunity against even claims based on the companies' own promises. Consider a standard online EULA or Terms of Use contract. That contract can impose strict controls on the consumer, on pain of copyright infringement and statutory damages. But the return promises of the company to keep the network safe or to provide accurate reputational information regarding other users of the network may well be largely unenforceable under CDA § 230.[203]

The advent of Mixed Reality technologies will aggravate this liability imbalance significantly. Again, the core example is mobile technology that can recognize another person and then report reputational data to the user.

199. *Id.* at 379 (citing § 230(c)(1) and stating that it effectively grants "operators of Web sites and other interactive computer services broad protection from claims based on the speech of third parties").

200. Android's application programming interface ("API") allows developers to use a code feature called RatingBar which allows them to assign a default star rating for an app. *See RatingBar*, ANDROID DEVELOPERS, http://developer.android.com/reference/android/widget/RatingBar.html (last updated Oct. 27, 2011).

201. *See, e.g.*, *Google Moves To Delete 'RuFraud' Scam Android Apps*, BBC NEWS (Dec. 14, 2011), http://bbc.in/GSOqNl.

202. *See* Ardia, *supra* note 198, at 481 (analyzing statistics of decisions under § 230, concluding that "overall, defendants won dismissal in 76% of the cases studied").

203. *Id.* at 493 ("[D]efendants won dismissal on section 230 or other grounds in more than three-quarters of the cases studied.").

Facial recognition technology is already being built into mobile devices.[204] And such technology does not merely recognize the device's user, but it can also recognize people in photographs that the user takes. Technologies like Face.com's facial recognition software are already combing online photo albums and identifying anyone who appears in the photographs.[205] Google+'s picture and video uploads are particularly aggressive—if the user is not cautious with permissions, Google+ will automatically upload pictures and movies from the user's telephone, and all future pictures and videos will be auto-uploaded.[206] Facial recognition is a standard mixed reality application, in that it takes indicia from the environment (here, the target face) and augments it with data (here, the person's reputation). The confluence of facial recognition, reputation, and mobile technologies will push problems of online reputation down to the personal level. Where once an employer had to be at a desk to Google your online reputation or check your social networking sites, now facial recognition will seamlessly integrate the process of online reputation into real life. Without progress in the law, the current legal framework governing reputation networks will replicate the same perverse incentives for Mixed Reality reputation systems that it has generated for online reputation networks. Consumers will bear a disproportionate amount of liability pursuant to the EULAs and TOUs of Mixed Reality applications, while their creators will largely be immune from liability.

C. PROPERTY LAW: THE DIGITAL LAND WARS

Mixed Reality augments real world objects, places, and people with virtual experiences. The augmentation of objects and places necessarily implicates property law. Imagine that someone "augments" your house with a virtual tag that contains an obscene word viewable through a Mixed Reality application. Can you assert rights as a property owner to remove the offensive virtual sign?[207] This Section tracks property shifts in response to technology and predicts shifts based on emerging Mixed Reality applications.

---

204. Biggs, *supra* note 183; Nick Bilton, *Facebook Changes Privacy Settings To Enable Facial Recognition*, N.Y. TIMES BITS (June 7, 2011, 4:30 PM), http://bits.blogs.nytimes.com/2011/06/07/facebook-changes-privacy-settings-to-enable-facial-recognition/.

205. *See* FACE.COM, http://face.com/ (last visited Feb. 19, 2012); *see also The Facial Recognition Software That Will Put a Name to Every Photograph in the Internet*, DAILY MAIL REP. (Aug. 23, 2010), http://www.dailymail.co.uk/sciencetech/article-1305191/Facial-recognition-software-allow-ability-identify-people-photographs-internet.html.

206. *Instant Upload Settings*, GOOGLE, http://www.google.com/support/mobile/bin/answer.py?answer=1304820 (last visited Aug. 14, 2011).

207. *See* John C. Havens, *Who Owns the Advertising Space in an Augmented Reality World?*, MASHABLE (June 6, 2011), http://mashable.com/2011/06/06/virtual-air-rights-augmented-

One perennial feature of the digital landscape is that of the digital land war.[208] The cycle goes as follows. First a range of options for the location of information is proposed. There is a divergence, and many different locations, applications, or networks are considered candidates for the "best" piece of internet real estate. There is then convergence once one address, application, or network becomes the "best," and people shift attention to it. Once attention shifts to only one address, application, or network, legal battles then follow as the owners of pre-existing property rights try to take the prime pieces of internet real estate away from the people who bet on the right technology.[209]

For example, early in the Internet's development, there were a few different top-level domain names. Some of these were restricted, like .mil and .edu. Some were general, like .net, .org, and .com. It was not immediately apparent that a .com domain name would become the most valuable piece of land on the Internet. It was only after the cycle of divergence—multiple top-level domain names existed—and convergence—to the .com domain name as the first choice of the searching consumer—that the legal wars over the .com domain names began. When they did, they did so in earnest, with Congress enacting legislation in support of the rights of trademark owners,[210] allowing them to take domain names from people who had registered them. The Anticybersquatting Consumer Protection Act permits the owner of a registered trademark to take a domain name that references the mark away from the registering party.[211] This permits trademark owners to wipe out free riding by parties who wish to use the trademark to sell goods, but it also gives the trademark owner another tool to quell critics of the trademark owner, or critics of the goods and services that the owner sells.[212]

---

reality/ (noting that "[m]ultiple apps feature the ability for ads to appear on your mobile screen as miniature virtual billboards assigned to GPS coordinates").

208. *See supra* note 25.

209. *See* Lipton, *supra* note 25, at 448.

210. *See* Trademark Act of 1946, Pub. L. No. 79-489, 60 Stat. 427 (codified as amended in scattered sections of 15 U.S.C.).

211. Pub. L. No. 106-113, § 1000(a)(9), 113 Stat. 1501, 1536 (1999) (enacting into law § 3002 of the Intellectual Property and Communications Omnibus Reform Act of 1999, S. 1948, 106th Cong., reprinted at 113 Stat. 1501A-545 to -548 (1999) and codified as amended at 15 U.S.C. § 1125(d)).

212. *See* Susan Thomas Johnson, *Internet Domain Name and Trademark Disputes: Shifting Paradigms in Intellectual Property*, 43 ARIZ. L. REV. 465, 476 (2001) (listing various types of cybersquatters, including one "who registers a domain name using the same or a *very* similar version of another entity's name to harass or criticize that entity" and "one who *intentionally* appropriates a famous trademark or tradename as a domain name for financial gain").

These land wars are far from settled. Another wave of land battles occurred over the use of metadata—mechanisms to drive customers to one site or another via search engine optimization.[213] Another modern-day wave is "Twitterjacking."[214] As Twitter became a social networking phenomenon, certain Twitter handles became valuable property. Immediately following the BP Gulf oil spill in 2010, some enterprising individual registered the handle "BPGlobalPR" and began a series of sardonic, self-involved, and hilarious tweets supposedly on behalf of BP.[215] It is not immediately clear that BP has the right to any Twitter handle that contains its name, especially ones that are being used for parody, or to convey truthful critical consumer information to the market.

The land wars continue in the sphere of Mixed Reality. For example, land wars are currently being waged over geolocated data tags. Yelp, a company that places GPS-located tags on businesses, includes reviews from ostensible customers. Litigation is now pending in New York against Yelp. The plaintiffs' goal is to force Yelp to remove negative reviews and stop removing positive reviews that are geotagged to the plaintiffs' businesses.[216] Furthermore, some European countries have voiced unrest because of the lack of control over the virtual representations of houses and property in Google Earth and through Google Maps.[217]

A coming wave of digital land wars will likely involve mirror worlds. Mirror worlds are virtual worlds that mirror the real world. The full 3-D version of Google Earth is a good example. With the latest software, consumers can see 3-D representations of buildings and view real-time relays

213. *See* Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 9 YALE J.L. & TECH. 111 (2006); *see also* David Segal, *The Dirty Little Secrets of Search*, N.Y. TIMES (Feb. 12, 2011), http://www.nytimes.com/2011/02/13/business/13search.html.

214. *See* William Sloan Coats & Jennifer L. Co, Kaye Scholer LLP, *The Right of Publicity & Celebrity Licensing*, 1065 PLI/PAT 277, 298 (2011) (describing Twitterjacking as the phenomenon of someone creating a Twitter feed and pretending to be a famous individual).

215. *See* Noam Cohen, *For Dueling BP Feeds on Twitter, Biting Trumps Earnest*, N.Y. TIMES (June 7, 2010), http://www.nytimes.com/2010/06/07/business/media/07link.html.

216. *See* Reit v. Yelp!, Inc., 907 N.Y.S.2d 411 (Sup. Ct. 2010).

217. *See, e.g.*, Catherine Bolsover, *German Foreign Minister Joins Criticism of Google's Mapping Program*, DEUTSCHE WELLE (Aug. 14, 2010), http://www.dw.de/dw/article/0,,5910738,00.html (describing complaints against Google Maps in Germany); *Google Street View Blacked Out in Greece*, CNN (May 13, 2009), http://articles.cnn.com/2009-05-13/world/greece.google.street.view.blocked_1_google-earth-search-giant-google-maps (describing the same in Greece); *Call To 'Shut Down' Street View*, BBC NEWS (Mar. 24, 2009), http://news.bbc.co.uk/2/hi/7959362.stm (describing the same in the United Kingdom).

from cameras at specific locations.[218] Fights over data tagged mirror worlds will be intense. Imagine if a global anarchist protest movement grabbed the mirror world location of local Wal-Mart stores and targeted them for mirror world protests by tagging the GPS location with anti-Wal-Mart facts and slogans; or imagine if members of the Occupy Wall Street movement tagged the locations of Wall Street firms with accusations and criticisms.[219] Consider the virtual defacing of a political headquarters in lieu of the more traditional brick through the window.

The land wars leave open a number of legal questions. The first question is whether owners of intellectual property rights—here, generally trademark owners—should be permitted to take prime internet locations away from first movers. Second, and more significantly, the land wars leave open the question of whether intellectual property law is itself the correct legal framework to apply.

The law of intellectual property tends here, as elsewhere, to exacerbate the trend towards increasing corporate control at the expense of protecting individuals. For example, imagine that a user Twitterjacks @Fairfield and begins to tweet as this Article's author. The author does not have the kind of celebrity that would give rise to a misappropriation of likeness claim, nor trademark or other IP ground on which to assert a claim to ownership of this new internet real estate. Yet Fairfield Inn & Suites would have a reasonable expectation of success in seizing the Twitter designation from a new registrant if someone were to register @Fairfield and begin tweeting hotel deals.[220] Thus, while I must register @Fairfield preemptively to protect my online persona, intellectual property owners often have the luxury of waiting to see which emergent technologies become dominant and then moving to secure the most valuable digital real estate. This gives IP holders a significant advantage.

Mixed Reality will only intensify the trend towards corporate control. As Mixed Reality causes real and virtual experiences to converge, there is a serious risk that the "virtual" rights holders (IP owners) will prevail and that "real" rights holders (real people and owners of physical property) will lose

218. *See Google Maps*, GOOGLE, http://maps.google.com (last visited Oct. 31, 2011) (containing a drop-down menu that enables the viewing of various live camera feeds in areas all over the world).

219. *See Occupy Movement (Occupy Wall Street)*, N.Y. TIMES, http://nyti.ms/AmZh25 (last updated Feb. 13, 2012) (containing articles chronicling the anti-Wall Street movement and the accompanying protests).

220. *See Trademark Policy*, TWITTER, https://support.twitter.com/groups/33-report-a-violation/topics/148-policy-information/articles/18367-trademark-policy (last visited Aug. 14, 2011).

out. Further, Mixed Reality is inherently a multi-channel exercise: which applications and which channels within those applications will become dominant is anyone's guess.[221] However, once an application or channel does become dominant, those users who first adopted a technology run the risk of being sidelined in favor of IP holders. And interestingly enough, real property owners—the owner of the hypothetical defaced house in the example above, for instance—do not have any such strengthened rights regarding their real world property.[222]

D. PRIVACY LAW: PRIVACY'S DEATH AND RESURRECTION

The advent of mobile computing has enabled the totalitarian dream (or nightmare) of tracking citizens at all times. For the most part, however, it is not the government that tracks citizens. Tracking is largely accomplished through the technology consumers themselves use.[223] Tracking technology is rampant and widespread. Google Streetview cars captured unencrypted personal data as the cars passed private homes.[224] Facebook initiated an open architecture for its developers that permits almost anyone to capture large amounts of information through an app installed by a friend of a friend.[225] GPS-enabled cell phones constantly record the real-world locations of their users.[226] Internet service providers do the same, tracking their customers across the digital landscape.[227] It follows that mobile broadband providers can not only track users' physical locations, but also correlate those locations with the users' online browsing habits.

---

221. *See* Havens, *supra* note 207 (suggesting that Google Goggles will be a dominant player given Google's current dominant market position).

222. *See id.* ("Google will own the virtual air rights within Goggles.").

223. *See* CHEN, *supra* note 6, at 47 ("[A]rmed with a camera-equipped smartphone and live streaming-video software, every citizen will have the power to broadcast anything to the world in real time, thus creating a collectively omniscient society of watching eyes.").

224. *See* Kevin J. O'Brien, *Germany Asks Apple About iPhone's Data Gathering*, N.Y. TIMES (June 28, 2010), http://www.nytimes.com/2010/06/29/technology/29apple.html ("[I]t had improperly collected 600 gigabytes of personal data, including fragments of e-mail messages and unencrypted passwords, on individuals around the world as it scanned home Wi-Fi networks while it gathered information for its Street View map archive.").

225. *See* Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, WALL ST. J. (Oct. 18, 2010), http://on.wsj.com/xVVPKF (describing how Facebook apps violate user privacy).

226. Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES (Mar. 26, 2011), http://www.nytimes.com/2011/03/26/business/media/26privacy.html (discussing the practice of how cell phone providers track users' latitude and longitude).

227. *See* Peter Whoriskey, *Every Click You Make*, WASH. POST (Apr. 4, 2008), http://wapo.st/xpbudQ (describing the growing phenomenon of internet service providers tracking individuals' online activity).

Likewise, even our friends and family can track us using widely available technology. As soon as one person takes a photograph and uploads it to Facebook, facial recognition technology can recognize and tag the people in the photograph with metadata (often including date and real-world physical location).[228] The government need not do much more than ask for this information from the mass of third parties who have already collected and indexed it.[229]

A discussion of online privacy is necessary in the context of Mixed Reality because Mixed Reality technology permits companies and governments to know not only a person's digital profile, but also his real-world habits.[230] There is nowhere to hide. Offline, real-world activity is now coded and recorded, parsed, and re-sold—thanks to the integration of Mixed Reality applications in our everyday lives—just as online activity has been. Where I drive every day can be cross-compared to my web surfing habits.[231] Where a consumer walks during the day is as marketable as which websites she has visited—and a combination of the two is more potent still.

Mixed Reality makes privacy increasingly elusive and unattainable. In fact, some urge that those who care about privacy should give up networked technologies. Former Google CEO Eric Schmidt implied that users who do not want to be tracked by Google all across the Internet, including any site that serves Google ads reporting back to Google, should simply not use the Internet.[232] Thus, in more recent years the move by privacy advocates has

228. *See* Lauren Effron, *Facebook in Your Face: New Facial Recognition Feature Raises a Few Eyebrows*, ABC NEWS (June 10, 2011), http://abcn.ws/wFWrBG (describing Facebook's facial recognition feature).

229. *Cf.* Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2325 (2008) (explaining the massive surveillance power of individuals resulting from the proliferation of cameraphones coupled with widespread mobile phone usage, and noting that cameraphones function as "sensors hooked into end-user devices"); *see* Mark Milian, *U.S. Sent Google 8,888 Requests for User-Data in 2010*, CNN TECH (June 27, 2011, 6:49 PM), http://www.cnn.com/2011/TECH/web/06/27/google.data.requests/index.html.

230. *See* Cohen, *supra* note 226 ("One product, CitySense, makes recommendations about local nightlife to customers who choose to participate based on their cellphone usage. Many smartphone apps already on the market are based on location but that's with the consent of the user and through GPS, not the cellphone company's records.").

231. *See* Andrew Munchbach, *Apple Sued over iPhone Location Tracking Scandal*, BGR (Apr. 25, 2011), http://www.bgr.com/2011/04/25/apple-sued-over-iphone-location-tracking-scandal/.

232. *See* Jared Newman, *Google's Schmidt Roasted for Privacy Comments*, PCWORLD (Dec. 11, 2009), http://www.pcworld.com/article/184446/googles_schmidt_roasted_for_privacy_comments.html (quoting Schmidt as stating, "[i]f you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time . . . .").

been to move some activity off the grid, or at least out of the reach of datamining corporations.[233] The advent of Mixed Reality technologies forecloses even this option.

1. Privacy Is Dead, Long Live Privacy

The ubiquity of technology that constantly tracks consumers' realspace movements and cross-references them with online activity has caused government and corporate actors to declare that "privacy is dead."[234] This Section explores the questions of whether privacy is in fact dead, whether Mixed Reality and mobile computing killed it, and what can be done about the current bleak situation. This Article takes the position that privacy is not an end state, but rather a point on a sliding continuum between secrecy and disclosure. Because privacy is a tension point, rather than an absolute category, it is inaccurate to state that privacy is dead.[235] Rather, the effects of mobile computing on privacy are a side effect of the nature of information systems used to locate, retain, and distribute information.

Since people will always seek to keep some information confidential and other people will always seek to discover or disclose it, we can quickly dispense with the "privacy is dead" paradigm. "Privacy is dead" is simply the battle cry of consumer disempowerment. To the extent privacy is dead, it is dead because the law has prevented consumers from getting and using the tools necessary to protect their personal privacy.[236] For example, it still is nearly impossible to surf the Internet securely,[237] or to make use of a cell phone without constantly revealing physical location or personal and

233. *See* Helen A.S. Popkin, *Privacy Is Dead on Facebook. Get Over It.*, MSNBC (Jan. 13, 2010), http://on.msnbc.com/xUnaGG.

234. *See* Newman, *supra* note 232; *see also* O'Brien, *supra* note 224 ("60 percent of households in Germany use a retail bonus card . . . . By participating, consumers give the company the right to collect and market data on their purchasing habits, as well as send them advertising."); Popkin, *supra* note 233.

235. *See* CHEN, *supra* note 6, at 188 (discussing how the conception of privacy has been forced to change and how the focus should be on developing new technologies to combat privacy concerns rather than simply decrying the existing framework); *see also* Nick Bilton, *Privacy Isn't Dead. Just Ask Google+*, N.Y. TIMES BITS (July 18, 2011, 12:59 PM), http://nyti.ms/GSOUTE (outlining how Google benefited by learning from privacy issues on Facebook and focusing on privacy concerns in Google+).

236. *See* Tanzina Vega, *Industry Tries To Streamline Privacy Policies for Mobile Users*, N.Y. TIMES MOBILE (Aug. 15, 2011), http://nyti.ms/yPYIj7 (describing positive developments on the privacy front as including "one company [that] is trying to make privacy policies that are both easy for consumers to read and easy for mobile application developers to create").

237. *See* John Markoff, *Do We Need a New Internet?*, N.Y. TIMES (Feb. 14, 2009), http://nyti.ms/GSOVHg; Kate Murphy, *New Hacking Tools Pose Bigger Threats to Wi-Fi Users*, N.Y. TIMES (Feb. 17, 2011), http://nyti.ms/GSOY5D.

financial information.[238] The goal, then, should be to provide consumers with the simple, built-in tools necessary to protect privacy.

2. Privacy by Design

The FTC has made much of "privacy by design."[239] This is an important meme to explore because it is both widespread and ineffective in securing privacy. Technologies that have been designed from the ground up to collect, package, and sell information cannot "by design" keep that information private. This Section explores the privacy by design meme, critiques it, and then discusses some more viable alternatives in the following Sections.

Privacy by design is an incorrect approach for two reasons.[240] First, the idea that privacy needs to be designed complicates a very simple problem. Corporations do not need to design for privacy because corporations do not need to record their customers' information in the first place. The need for privacy design arises only because the existing technologies have already been designed to gather and sell customers' information. Once one rephrases "privacy by design" as "designing systems and services with the purpose of collecting and disseminating information to not collect or disseminate information,"[241] the futility of the approach becomes apparent.[242] Thus, the first reason that privacy by design has not produced privacy online is because the technologies have been designed not to allow for privacy.

238. Angwin & Valentino-Devries, *supra* note 175; Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 705–06 (2011) (stating that if cell phone data of one individual were recorded, "it could create a . . . virtual map of all the places the person went and how much time he spent at each place along the way"); Ki Mae Heussner, *Apple Tracks Location with iPhone, iPad Data*, ABC NEWS (Apr. 20, 2011), http://abcn.ws/wghaeh (noting that the "Apple iPhone and iPad 3G record the device's geographic position and corresponding time stamp in a hidden file").

239. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (advocating that companies adopt "privacy by design" as a means of protecting consumer privacy by limiting disclosure of consumer data through product design).

240. For background on privacy by design, see generally Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1431–43 (2011) (describing various reasons why privacy by design has not enjoyed the amount of success anticipated).

241. Simply put, the technology today has been developed with collection of user data in mind. The privacy by design concept is seemingly contradictory because it would be used to enhance privacy in systems that have been designed specifically to gather consumer information.

242. *See* Klinefelter, *supra* note 177, at 18 (identifying major concerns, in particular for the legal community stemming from confidentiality, and the concerns raised by viruses, third parties, and other bad actors with regard to online research and data saved by third party tracking).

The second, and related, reason is that the privacy options that consumers do have are designed to be too expensive in terms of the time and attention required to use them.[243] For example, industry advocates continue to argue against regulatory enforcement of a browser "do not track" flag that would follow the model of the quite successful federal "do not call" list.[244] Instead, consumers must navigate a different privacy architecture for each application provider, online service provider, and software developer. Drawing an analogy to the telephone context is instructive. Prior to the do-not-call list, each telemarketer was required to maintain and honor lists of people who did not wish to be contacted. Yet the sheer weight of informing each telemarketer (never mind the telemarketers who ignored the rules) made it such that telemarketing was hardly impacted. A unified, simple do-not-call list permitted consumers to express their preferences just once, rather than serially on the phone serially with each one of a thousand different callers.

Privacy by design is to some degree contradictory because the current commercial data architectures are in fact mechanisms for collecting, packaging, and reselling consumers' private and personally identifiable data.[245] Further, the privacy options that online users do have are designed to exhaust and confuse the user by requiring them to understand and address their privacy concerns with each vendor separately.[246] Privacy by design is a system designed not to work.

3. Privacy as Control

The solution to the privacy problem is simple, default, universal, and legally enforceable consumer controls for privacy. Consumer control is not only necessary; it is an effective solution in light of changing consumer conceptions with regard to privacy. Consumers are coming to treat privacy as a matter of control rather than an absolute prohibition on disclosure.[247] A consumer control regime would, as it should, allow consumers to sell their

243. *See* Vega, *supra* note 236 (discussing the difficulty with online privacy policies, the importance of privacy policies on data collection, and the growing concern over data collection).

244. *See* David Goldman, *FTC 'Do Not Track' Plan Would Cripple Some Web Giants*, CNN MONEY (Dec. 3, 2010), http://money.cnn.com/2010/12/02/technology/ftc_do_not_track/index.htm (identifying several industry leaders, such as Google, who are against "do not track" due to unforeseen security problems and loss in e-commerce and advertising revenues).

245. *See* Rubinstein, *supra* note 240, at 1412 (noting that the profits derived from online advertising make firms reluctant to voluntarily impose systems that will increase consumer privacy to the detriment of their ability to collect consumer information).

246. *See* Vega, *supra* note 236.

247. *See* CHEN, *supra* note 6, at 188; Bilton, *supra* note 235 (praising Google+ for its default privacy settings).

personal information and allow internet companies to use it.[248] If implemented, effective consumer-side privacy controls can provide a true market in information.

Additionally, the decision as to whether or not to permit online or offline tracking can more easily and effectively reside in the customer's hands. This is clear in light of the unworkable alternatives to consumer control of privacy. The current regime of privacy policies (that contain no privacy protections) and EULAs (that bury invasive privacy terms twenty pages deep in electronic documents) has proved unworkable. Similarly, leaving privacy controls in individual companies' hands has proven to be a longstanding fox-in-the-henhouse type failure.

Implementing a consumer control regime would be relatively easy. A simple, expedient solution such as legally enforcing the "do not track" flag already available in browsers would do the trick. A consumer-side "do not track" option would test the economic arguments of privacy naysayers. These naysayers argue that there is no privacy because consumers do not want it, or at least that consumers want products more than privacy.[249] For example, Eric Schmidt has stated in relation to Google Streetview that "[i]f you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[250] Milder versions of the same strange argument include the assertion that consumers who do not wish to be tracked are free to not use Google, or are free not to use the Internet, or are free not to use the telephone. And with the advent of mobile computing technology, we might say that a consumer who does not wish to be tracked and recorded is free not to leave her house.

The market for consumer privacy has yet to be tested because "privacy by design" policies shift all of the transaction costs of privacy onto consumers. To discover what consumers make of privacy online, the transaction costs of privacy should be shifted from consumers to the owners of internet technology. Shifting the transaction costs from consumers and

248. *See* Vega, *supra* note 236 (harmonizing the needs of users with the needs of companies to create a balance on the privacy front, but noting how online advertising reduces the costs of mobile applications). Mobile apps are free or cheap largely because of mobile advertising. *See also* Jim Harper, *The Great Privacy Debate—It's Modern Trade: Web Users Get as Much as They Give*, WALL ST. J. (Aug. 7, 2010), http://on.wsj.com/ArHG25 ("The reason why a company like Google can spend millions and millions of dollars on free services like its search engine, Gmail, mapping tools, Google Groups and more is because of online advertising that trades in personal information.").

249. *See* Harper, *supra* note 248 (arguing the same point on behalf of consumers in that protections for consumers would invite them to abandon personal responsibility).

250. *See* Newman, *supra* note 232.

offering consumers simple and legally enforceable control over online and offline privacy would also test the argument advanced by some in the internet technology industry that citizens do not want privacy.[251] And if internet technology companies like Google refuse to respect consumers' privacy settings, companies will have the choice to not offer service to those consumers.

A true market for privacy requires customers to have market choices that are not overwhelmingly burdened by transaction costs. The self-regulating approach to the private information market in the United States characterized by decentralized, complex, and unenforceable privacy controls has resulted in full market failure. Simple, legally enforceable, default consumer-side browser-level protections for consumers will remedy this problem by centralizing decision-making in consumers, rather than in corporations or the government.

Privacy as control represents an alternative to privacy by design.[252] Privacy as control assumes that consumers have effective, unitary, and legally enforceable controls in their own hands,[253] rather than scattered, complex controls that vary according to each service provider.[254] This vision of true consumer control over privacy is particularly important in the Mixed Reality context. Without real control over information, consumers will be every bit as subject to constant tracking in their real lives as they are now in their online habits.

IV. BALANCED LAW FOR MIXED REALITY

Mixed Reality merges the real world and cyberspace. It presents exciting opportunities for consumers to augment realspace with rich virtual experiences. But the merging of real and virtual worlds also presents a basic legal problem. Law online has ventured far away from its offline roots. There is a very real risk that as virtual and real merge, the law intended to govern

251. *See* Rubinstein, *supra* note 240, at 1412 (listing various reasons why consumers may not want privacy, such as lack of knowledge, behavioral biases, or simply not caring about the issue).

252. *See* CHEN, *supra* note 6, at 188–89 ("Perhaps we have already given up our digital privacy, but we still have control over boundaries . . . . In a modern online context a violation of privacy may only occur when we are manipulated into sharing more than we were told we would be sharing.").

253. *See* LAWRENCE LESSIG, CODE VERSION 2.0, at 88–111, 228–30 (2006) (arguing for a property model to protect privacy).

254. *See* CHEN, *supra* note 6, at 189 ("Online privacy advocates criticize online services when they are unclear or dishonest about what they are doing with our data, not when they are using our data—because, of course, they are.").

intangible assets will come to govern everyday life.[255] The law governing intangible assets was not designed to apply to the real world. If and when it is applied to the real world, the result will be extremely problematic. The specialized law of intellectual property and online contracting is not the best rule set from which to draw rules about everyday human life. Real world analogies, not online analogies, are the best source for legal rules governing the convergent technology of Mixed Reality.[256]

Solutions that have proven useful in law historically should be applied to the emerging legal problems generated by Mixed Reality.[257] The law has long-evolved internal checks and balances. For example, the common law has long imposed restrictions on how much control an intellectual property owner may assert once she has sold a product.[258] Similarly, the law has long set basic limits on contracts—limits that should be given new life in the online context generally, but also particularly in the context of Mixed Reality. Very little is needed to solve one of the major problems, that of protecting consumers' data. Here the law need only enforce consumers' expressed preferences to maintain their privacy and reject the pernicious myth of consent to the sale of personal information. Simple, unitary, default, and legally enforceable privacy controls will generate a much better market in consumer information.[259] The following Sections demonstrate through three examples that the law of intangible assets applied online should not be applied to Mixed Reality applications.

---

255. *See* Boone, *supra* note 53, at 114–15 (detailing that underlying code is what controls a virtual world). *See generally* CHEN, *supra* note 6 (describing how the iPhone collapsed the physical and virtual world); Barfield, *supra* note 5, at 161 (describing advertising in augmented reality); Gross, *supra* note 11 (describing an augmented reality mobile application); Wilson, *supra* note 52, at 1133 (describing the potential of near field communications).

256. *See* Lyria Bennet Moses, *Recurring Dilemmas: The Law's Race To Keep Up with Technological Change*, 7 U. ILL. J.L. TECH. & POL'Y 239, 279–80 (2007); *see also* Perzanowski & Schultz, *supra* note 158, at 892.

257. *See* Fairfield, *supra* note 8, at 475–76 ("For online communities to thrive, courts must recognize that private property, torts, and other community-critical rights and obligations can be adapted from the familiar rules that already govern communities in the real world to suit the realities of the virtual world.").

258. *See* Perzanowski & Schultz, *supra* note 158, at 892 ("[C]opyright exhaustion, like many principles recognized in the Copyright Act, was created by and should continue to develop through common law judicial reasoning.").

259. *Cf.* Eric J. Feigin, *Architecture of Consent: Internet Protocols and Their Legal Implications*, 56 STAN. L. REV. 901, 902 (2004) ("Higher-level protocols, such as those utilized in most web interactions, involve exchanges that should be considered express consent: the formation of a legally binding contract.").

A. CONSTRAINING INTELLECTUAL PROPERTY

The first and largest problem that this Article has identified is that as virtual and real legal interests merge, the law appears set to grant far greater rights to intellectual property holders than it does to holders of other legal rights, like personal dignity or real property.[260] Copyright law is the main culprit, but other areas of intellectual property are also at fault. For example, as seen in Section III.C, *supra*, owners of trademarks have a decided advantage in the race for prime online real estate.[261]

The law has already developed checks on the ability of an intellectual property holder to exert continuing control over its customers once it has sold its product, but courts have not applied these checks to online law.[262] Copyright is meant to prevent copying. Once a copy is sold however, a copyright owner no longer has the power to control the copy. This is the common law doctrine of "first sale," which has been enshrined in the Copyright Act.[263] The doctrine hinges on whether a copyrighted work has been "sold" or merely "licensed." The answer to this question is complex, and courts rarely get it right. Again, online law has diverged strongly from offline law. For example, although Netflix can buy a physical DVD and rent it out to any customer (thus ensuring that almost any program or movie is available through Netflix's mail service), Netflix must seek individual license deals on a per-provider basis in order to stream the very same content. Thus, while Netflix's ability to use the physical copy of the same movie is not restricted, its ability to utilize an online copy is curbed by licensing and copyright law—in this case, the IP holder has much more power over the online version.

There is, however, one interesting development. Courts seem to draw a distinction between electronic data that is recorded or embedded in a physical medium, and data that is merely free flowing.[264] This is an improper

260. *See* Lemley, *supra* note 139; *see also* sources cited *supra* note 255.

261. *See* text accompanying *supra* notes 211–12.

262. *See* 17 U.S.C. § 106(1) (2010) (giving the exclusive right to reproduce work that is copyrighted). *But see id.* § 117(a)(1) (providing for the essential step defense for the software context where an owner of a lawful copy does not infringe the reproduction right of the copyright owner if the reproduction is an essential step in the utilization of the software); *id.* § 109(a) (providing for the first sale doctrine where a lawful owner of a copy of a copyrighted work is able to sell or otherwise dispose of the possession of the relevant copy at the owner's discretion). Both of these affirmative defenses are limited to owners of lawful copies of copyrighted works.

263. § 109(a).

264. *See* RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 U.S. Dist. LEXIS 1889, at *1, *3 (W.D. Wash. Jan. 18, 2000) ("Streaming is to be contrasted with 'downloading.' ").

distinction from a functional point of view: there is no relevant distinction between a song encoded on a CD and a song downloaded as an MP3. Yet courts continue to apply real world physical analogies to digital goods embedded in physical objects and apply the law of intangible assets to digital goods that are not so embedded. Thus, while a consumer may record movies on her TiVo, there is a serious question as to whether she may record a streaming movie with a virtual VCR.[265] Similarly, recent cases in the Ninth Circuit indicate that although a seller may not resell copies of a computer program on e-Bay (since the original license agreement purported to prohibit such resale),[266] she would be free to sell music CDs that purported to have the self-same restriction.[267] The presence of some physical element—here the TiVo physical box or the music CD—seems to provide courts with some comfort that analogies to the law of the sale of physical objects is a better analogy than the law of licensing of intellectual property.

These cases may provide a ray of hope for Mixed Reality. Although the data is tied and not embedded, there is hope that the link to the real world may make courts more likely to use analogies drawn from the full range of law, rather than analogies drawn solely from online intellectual property law.[268]

B. LIMITING ONLINE CONTRACTUAL CONTROL

The second step to returning balance to the law as cyberspace and realspace merge is to restore balance to online contract. Reducing the application of intellectual property law and increasing the application of traditional principals of contract and property law can largely restore balance in online contracts.[269] This will return contract law to its normal place within the constellation of legal tools as the tool of bargained-for exchange and expectation damages.

---

265. *Id.* at *34–35 (halting Streambox's continuance of its product, a virtual VCR). *But see* Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 128 (2d Cir. 2008) ("Accordingly, we construe *MAI Systems* and its progeny as holding that loading a program into a computer's RAM *can* result in copying that program. We do not read *MAI Systems* as holding that, as a matter of law, loading a program into a form of RAM *always* results in copying.").

266. *See* Vernor v. Autodesk, Inc., 621 F.3d 1102, 1110–12 (9th Cir. 2010) (establishing a three point framework to determine if a purchaser of software is an owner or licensee).

267. *See* UMG Recordings, Inc. v. Augusto, 628 F.3d 1175, 1183 (9th Cir. 2011) (finding resale of a music CD not to constitute copyright infringement despite a label claiming a license limitation restricting such a sale).

268. *See* Moses, *supra* note 256.

269. *See* Lyria Bennet Moses, *Toward a General Theory of Law and Technology: Why Have a Theory of Law and Technological Change?*, 8 MINN. J.L. SCI. & TECH. 589, 595–96 (2007) ("Over-emphasis on the technological angle in discussing legal and social problems is evident in various contexts. . . . Judges occasionally fall into the same trap of assuming that because events took place on the Internet, the law must be different.").

As things stand, online contracts often implicate intellectual property statutory damages that have no relation to actual damages. For example, when a user modifies her physical gaming console in violation of an EULA, the console seller can pursue statutory damages for direct and vicarious copyright infringement. However, if traditional principles of contract law applied, the console seller would be limited to contract damages. The latter approach follows logically because the gamer owns her console and should be able to do with it what she will.

A return to basic principles of contract law has also generated promising trends elsewhere in the law. A related area in which intellectual property control over contracts is being scaled back is in circuit courts' interpretations of the Digital Millennium Copyright Act ("DMCA").[270] Here, the intersection between contract and copyright occurs in the anti-circumvention systems used to protect the copyrighted materials. A click-through contract (the classic "click *I Agree* or exit") can serve as both a binding contract and as a technological protection measure,[271] since the content governed by the contract cannot be accessed without going through the contract.

If the DMCA's prohibition on circumvention of such protective measures is relaxed, users can make use of their programs on their own devices despite overreaching contract terms. Interestingly, here too courts have been persuaded by analogies to physicality to relax the prohibitions of the DMCA.[272] Whereas hacking into a purely electronic software program seems to be a clear violation of the DMCA,[273] bypassing protections embedded into physical objects receives more lenient treatment. Indeed, the Library of Congress recently added anti-circumvention exceptions to the DMCA that would allow users to alter their smartphones to use unofficial but legally-obtained software.[274] The Court of Appeals for the Sixth Circuit

270. DMCA, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.). The DMCA contains three provisions that create a framework to address circumvention of technological measures that protect copyrighted works. *See* 17 U.S.C. § 1201(a)(1)–(2), (b)(1) (2010).

271. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996); *see also* 17 U.S.C. § 1201(a)(1)(A) ("No person shall circumvent a technological measure that effectively controls access to a work protected under this title.").

272. *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 529 (6th Cir. 2004); Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203–04 (Fed. Cir. 2004).

273. § 1201(a)(1)(A).

274. *See* Paul Miller, *Library of Congress Adds DMCA Exception for Jailbreaking or Rooting Your Phone*, ENGADGET (July 26, 2010, 11:33 AM), http://www.engadget.com/2010/07/26/library-of-congress-adds-dmca-exception-for-jailbreaking-or-root/ (noting the Library of Congress's exception to the DMCA).

held that circumventing controls that limited the number of times that a user could refill printer cartridges that she had purchased was not a violation of the DMCA.[275] Similarly, the Federal Circuit held that a universal garage door opener that bypassed the garage door manufacturer's rolling numeric access code did not trigger the sanctions of the DMCA.[276] It may seem obvious that universal remotes do not violate anti-hacking laws, but legally speaking the issue is an extraordinarily close one, since software is embedded in the remote. Courts' willingness to give weight to the consumer's expectation that a garage door would be compatible with universal remotes over the strict letter of the DMCA affirms the importance of consumers' property rights and expectations with respect to their own property.

Two ancient but basic limits on overreaching contractual control are slowly coming back into fashion online: consideration and its cousin, illusoriness. The common law has long declined to look into the value of a particular bargained-for exchange, but has instead used the doctrines of consideration and illusoriness to ensure that some bargain was indeed struck—that promises were made on both sides.[277] But in the online context it is not clear that enforceable promises are being made on both sides. EULAs and TOUs are lists of promises that the user makes. Ostensibly, the return promise by the corporation is that it will permit the user to access a valued service. But courts are increasingly questioning contracts that contain unlimited modification clauses.[278] These are a staple of online contracts, but they are becoming more and more dangerous for companies. Judges have begun to reason that if a company is free to change the EULA or TOU at any time and in any way, then the company has not made any true return promise.[279] This is an important legal development since it increases the odds that the contract to which a consumer agrees will state the actual responsibilities that may eventually be enforced against the consumer. Similarly, such legal rulings increase consumers' confidence that the return promises of the company are equally enforceable.

Constraining overreaching contracts—especially those contracts that forbid the user to customize or accessorize her own property—is essential for Mixed Reality. Mixed Reality devices will increasingly control how users

275. *Lexmark*, 387 F.3d at 529.

276. *Chamberlain*, 381 F.3d at 1182.

277. *See* Harris v. Blockbuster Inc., 622 F. Supp. 2d 396, 397–400 (N.D. Tex. 2009) (holding that an arbitration clause was illusory because the drafter could alter it at will).

278. *See, e.g.*, Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 611 (E.D. Pa. 2007) (finding that a unilateral modification provision was unconscionable).

279. *See* Morrison v. Amway Corp., 517 F.3d 248 (5th Cir. 2008).

view the world around them. They are the access point for users' ability to see the data-enriched experiences that augment real places, people, and things.[280] The devices that control Mixed Reality experiences must be firmly in citizens' hands. Owners of Mixed Reality devices must be able to modify those devices in order to control the reality that they experience. The alternative is imaginable but unthinkable: just as Sony now claims that it has the sole right to control what players experience via its gaming console, on pain of criminal sanction and intellectual property infringement, so Mixed Reality providers would claim the ability to control the very reality that citizens experience and share.

C. RETURNING CONTROL OVER PRIVACY TO CONSUMERS

In the privacy context, a very simple but fundamental rebalancing of contract law as applied online will resolve many problems. Privacy is handled as a matter of contract under U.S. law.[281] That is not the problem. The problem is that the law of contract as applied online has denied consumers the power to draft contracts. Even in the strangest circumstances, courts enforce contracts written by corporations, including legal language contained on pages that the user has not even seen.

Yet that reasoning ought to cut both ways. Citizens—as parties to a contract—have as much of a right to add binding terms to a contract as corporations do.[282] If a consumer sets a "do not track" flag in her browser, courts should enforce it as a matter of contract law. Courts have long held that consumers "agree" to online contracts by continuing to use a website or online service.[283] It would be nonsensical not to apply the same logic to a

280. *See* CHEN, *supra* note 6; Bilton, *supra* note 89; Glusac, *supra* note 17; Husson, *supra* note 89; King, *supra* note 22.

281. *See* News Release, Fed. Trade Comm'n, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), http://www.ftc.gov/opa/2000/07/toysmart2.shtm (discussing the FTC's suit against Toysmart and the company's attempt to take action directly in violation of its privacy policy). Cases that have found otherwise only serve to emphasize the problem that lies in interpreting privacy as non-contractual. *See, e.g.*, *In re* Jet Blue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299 (E.D.N.Y. 2005); Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004). This does not, however, undermine the notion that the FTC still enforces privacy policies as promises to consumers.

282. *See* LESSIG, *supra* note 253; Feigin, *supra* note 259.

283. *See* Yen-Shyang Tseng, *Governing Virtual Worlds: Interration 2.0*, 35 WASH. U. J.L. & POL'Y 547, 556 (2011) ("Generally speaking, courts have tended to enforce all of these forms of licenses, even though the licenses may unilaterally impose one-sided terms with little to no room for negotiation.").

corporation: by continuing to provide service to a customer who has set a "do not track" flag, the corporation should be legally bound by that term.[284]

This proposal is of course not uncontroversial, but it exposes the poor reasoning underlying the law of online contracting.[285] Functionally speaking, under current law only corporations are allowed to draft online contracts. Citizens are only granted the pro-forma right to agree to pre-set corporate terms. Citizens are denied a voice in setting the terms under which their information is gathered.[286] It is this perverse state of affairs that we must correct before the law of online contracting can govern everyday life.

Giving consumers control does not mean that control should be complicated. To impose all of the transaction costs of privacy protection on consumers—the current state of affairs—is planned failure. In order for consumers to be able to express their preferences effectively, privacy controls must be simple, unitary (in one place, applicable to all counterparties), default, and legally enforceable.[287] Only under these circumstances will the transaction costs of private agreement over privacy be manageable for consumers. The alternatives are significantly less attractive: outright paternalistic government regulation on the one hand, or the current wild west of data protection on the other.

The advent of Mixed Reality technology makes this return to consumer control over personal data of significant importance. Consider the average smartphone, which comes pre-loaded with numerous apps, each of which has different permissions to track the consumer's real-world location, social network interactions, and even tap into the basic reality that the consumer is experiencing—what she is hearing and seeing.[288] Consumers must have control over their own reality, and this includes the ability to control their own information as it is propagated through these networks.

---

284. *See* LESSIG, *supra* note 253; Feigin, *supra* 259.

285. *See, e.g.*, Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1662 (2011) (noting various problems with trying to achieve privacy by consumer contracting).

286. *See* Newman, *supra* note 232; Popkin, *supra* note 233.

287. *See* LESSIG, *supra* note 253; Feigin, *supra* note 259; *see also* Séverine Dusollier, *The Master's Tools v. The Master's House: Creative Commons v. Copyright*, 29 COLUM. J.L. & ARTS 271, 272 (2006) (discussing the purpose of Creative Commons to address the "recent expansion of copyright" and how it is "overreaching and detrimental both for future creators and for the users of copyrighted works"); *About the Licenses*, CREATIVE COMMONS, http://creativecommons.org/licenses/ (last visited Feb. 19, 2012) (providing for a standard option set of contractual licenses that have revolutionized online exchanges).

288. *See* Yukari Iwatani Kane & Scott Thurm, *Your Apps Are Watching You*, WALL ST. J. (Dec. 17, 2010), http://on.wsj.com/wq7Wiw (describing how iPhone and Android transmit various data about the phone without the user's knowledge).

V. CONCLUSION

The proposals here are not exhaustive. Rather, they are examples of potential benefits to be gained through application of a method. That method involves applying the common law approach—reasoned, careful, limited, and iterative decision-making based on the closest legal analogy—in order to find potential solutions to emerging technological problems.[289]

Mixed reality tools are pushing intellectual property regimes into realspace. In some senses, this is nothing new. Books are real, and intellectual property governs our ability to copy them. But the law of intellectual property licensing online has drifted from its moorings. Offline, the law of copyright has generally been limited to restricting the ability of a buyer to make copies, perform unlicensed performances or screenings, or create non-parody derivative works. Not so online, where copyright law has the ability to control the social rules of multiple-million member online communities. Mixed Reality technology brings this online over-extension of copyright licensing back into everyday life.

As Mixed Reality merges virtual experiences with everyday life, there is a very real risk that courts will continue to draw on the law of online intellectual property licensing. The confluence of the judicial acceptance of pro forma corporate contracts coupled with the strength of contracts backed by out-of-proportion copyright infringement damages means that the law of online contracting and intellectual property licensing is a terrible fit for offline, everyday life.

In everyday life, when a consumer buys a car, the consumer expects to be able to paint it any color. Yet when a consumer buys a garage door, there is a non-trivial question of law as to whether the manufacturer of the garage door may force the consumer to buy new remote controls from only the garage door manufacturer. And when a consumer buys a Playstation 3, there are very real legal threats from Sony when the consumer modifies her own property and teaches others how to do the same.

This overextension of copyright licensing and online contracting law is undermining property rights in the real world, providing perverse incentives for online reputation purveyors to whitewash the reputations of network users, and burying consumers under thousands of differing privacy policies, many of which are not enforceable or which may be changed at any time by the software provider.

289. *See* Perzanowski & Schultz, *supra* note 158; *see also* Moses, *supra* note 256, at 241.

But there is hope. This Article proposes applying simple rules evolved in the full context of real-world situations to merged virtual and real experiences. A consumer's property interest in her goods should permit her to make aftermarket modifications of her own property. A copyright holder's rights in a given copy should be exhausted when the copyright holder sells a given copy away, never mind that the transaction is spuriously characterized as a license. And history has shown that consumers not only want privacy but can enforce their preferences quite effectively. However, consumers must be granted simple, unitary, and default tools that permit them to have an active say in the information gathering regimes to which they are subject, rather than the option to pick which one of a set of corporate-drafted terms they may agree to.

As Mixed Reality merges virtual and real space, it provides serious challenges to law, but also offers serious hope. The law of intellectual property as applied to the real world is subject to traditional constraints that render it much less problematic than the unconstrained law of intellectual property as applied to Mixed Reality. The law of contracting in the real world grants both parties, not just corporations, the ability to contribute terms to the contract. Consumers actually can police their privacy quite effectively, if given simple, opt-in, and default options to do so. Mixed Reality opens the door to the application of common sense rules that have very effectively mediated the tensions between corporation and consumer, citizen and state. Mixed Reality need not be a dystopian vision. It may be the method by which we can restore balance to the law.

CAN YOU SEE ME NOW?: TOWARD REASONABLE STANDARDS FOR LAW ENFORCEMENT ACCESS TO LOCATION DATA THAT CONGRESS COULD ENACT

Stephanie K. Pell[†] *& Christopher Soghoian*[††]

ABSTRACT

The use of location information by law enforcement agencies is common and becoming more so as technological improvements enable collection of more accurate and precise location data. The legal mystery surrounding the proper law enforcement access standard for prospective location data remains unsolved. This mystery, along with conflicting rulings over the appropriate law enforcement access standards for both prospective and historical location data, has created a messy, inconsistent legal landscape where even judges in the same district may require law enforcement to meet different standards to compel location data. As courts struggle with these intertwined technology, privacy, and legal issues, some judges are expressing concern over the scope of the harms, from specific and personal to general and social, presented by unfettered government collection and use of location data and how to respond to those harms. Judges have sought to communicate the scope and gravity of these concerns through direct references to Orwell's dystopia in *1984*, as well as suggestive allusions to the "panoptic effect" observed by Jeremy Bentham and his later interpreters, such as Michel Foucault. Some have gone on to suggest that privacy issues raised by law enforcement access to location data might be addressed more effectively by the legislature.

This Article proposes a legislative model for law enforcement access standards and downstream privacy protections for location information. This proposal attempts to (1) articulate clear rules for courts to apply and law enforcement agents and industry to follow; and (2) strike a reasonable balance among the interests of law enforcement, privacy, and industry with the ultimate goal of improving the position of all concerned when measured against the current state of the law.

---

† Principal, SKP Strategies, LLC; former Counsel to the House Judiciary Committee; former Senior Counsel to the Deputy Attorney General, U.S. Department of Justice; former Counsel to the Assistant Attorney General, National Security Division, U.S. Department of Justice; and former Assistant U.S. Attorney, Southern District of Florida. Email: stephanie@stephaniepell.net

†† Graduate Fellow, Center for Applied Cybersecurity Research; Ph.D. Candidate, School of Informatics and Computing, Indiana University. Email: chris@soghoian.net.

The authors would like to thank Derek Bambauer, Catherine Crump, Susan Freiwald, Jim Green, Albert Gidari, Markus Jakobsson, Paul Ohm, Christopher Slobogin, and Magistrate Judge Stephen Wm. Smith for their feedback and assistance. The authors would also like to thank the attendees of the Privacy Law Scholars Conference, where this Article was presented in the summer of 2011.

TABLE OF CONTENTS

I. INTRODUCTION

Over several months in 2008, a gang of five men, described as the "Scarecrow Bandits" in media reports, committed or attempted twenty-one violent "takeover-style" bank robberies in the Dallas area.[1] FBI agents investigating the case contacted cellular telephone companies and obtained phone number logs to determine which telephones had been near the banks around the time of the heists. By searching these voluminous records, agents discovered that two phones had made calls near twelve of the robbed banks.[2]

1. *See* Press Release, Dep't of Justice, Federal Jury Convicts Scarecrow Bandits on Bank Robbery and Firearm Offenses (Aug. 13, 2009), http://www.justice.gov/usao/txn/PressRel09/scarecrow_bandits_convict_pr.html.

2. *See* Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET NEWS (Feb. 11, 2010), http://news.cnet.com/8301-13578_3-10451518-38.html.

Similarly, after two men robbed a Connecticut bank in July 2008, law enforcement agents obtained historical cell tower logs revealing 180 different phone numbers that had made or received calls near the bank at the time of the robbery. Although these logs led police to two brothers, both of whom were soon arrested, the police also obtained and retained location information associated with 178 innocent people who will never learn that their phone companies disclosed information to police.[3]

Law enforcement agencies—already using location information in their investigations—are likely to increase their reliance on such information as technology improves.[4] This is true of requests for all types of mobile device location data, whether historical or real-time (prospective),[5] in conducting criminal investigations and locating fugitives. For example, primarily due to the use of location information, the average time needed for the U.S. Marshals Service to find a fugitive has dropped from forty-two days to only two.[6] In recent congressional testimony, a senior Department of Justice ("DOJ") official explained how a homicide detective and his partner in Prince George's County, Maryland, used "cell tower [location] information" to pursue a man wanted for a triple murder, capturing him in only nine hours.[7] Having this information "immediately accessible" allowed the marshals to deploy "available law enforcement resources [effectively] . . . without placing officers, or the public, at undue risk."[8] Clearly, location information has become a powerful investigative tool in support of a range of law enforcement responsibilities.[9]

---

3. *See* Declan McCullagh, *ACLU: FBI Used 'Dragnet'-Style Warrantless Cell Tracking*, CNET NEWS (June 22, 2010), http://news.cnet.com/8301-31921_3-20008444-281.html.

4. A more technical explanation of location information is presented *infra* Part II, but for purposes of this example, location information means information about or derived from a portable device, such as a cellular phone, that reveals the location of the device either approximately or with a high degree of precision.

5. McCullagh, *supra* note 2 ("Obtaining location details is now 'commonplace,' says Al Gidari, a partner in the Seattle offices of Perkins Coie who represents wireless carriers.").

6. *See Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 2 (2011) (statement of Dr. Susan Landau), *available at* http://judiciary.house.gov/hearings/pdf/Landau02172011.pdf.

7. *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing before the S. Comm. on the Judiciary*, 112th Cong. 5 (2011) [hereinafter *Senate Judiciary 2011 ECPA Hearing*] (statement of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice), *available at* http://1.usa.gov/IsojNy.

8. *Id.*

9. *See* Michael Isikoff, *The Snitch in Your Pocket*, NEWSWEEK (Feb. 18, 2010), http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html.

The tool proved so effective that the number of "requests"[10] to carriers for location information grew "exponentially" over the past few years, with major wireless carriers now receiving thousands of requests per month.[11] Sprint Nextel received so many requests that it developed a web interface that gave law enforcement direct access to its subscribers' location data.[12] Law enforcement agents used the website to "ping" Sprint subscribers over eight million times in a single year.[13]

Law enforcement's increased use of location information has spurred courts to scrutinize more closely government applications to compel third parties to disclose location data, as certain magistrate judges question and examine what legal standards govern law enforcement access to historical and prospective location information. Prosecutors "were using the cell phone as a surreptitious tracking device," Judge Smith, a federal magistrate in Houston, told a reporter from Newsweek. "I started asking the U.S. Attorney's Office, What is the legal authority for this? What is the legal standard for getting this information?"[14]

All law enforcement demands (not involving voluntary emergency disclosures) for location information, whether seeking historical or prospective data, require some type of court order authorizing a compelled disclosure.[15] Determining the proper access standard—whether the *higher* "probable cause" standard, the *lower* 18 U.S.C. § 2703(d) order requiring "specific and articulable facts" that the information sought is "relevant and

10. The use of the word "requests" in this context means both compelled disclosures of location information where law enforcement presents a third-party provider with a probable cause warrant or an 18 U.S.C. § 2703(d) order and voluntary emergency disclosures pursuant to 18 U.S.C. § 2702, where providers may voluntarily share information with law enforcement in the case of an emergency involving danger of death or serious physical injury to any person.

11. Isikoff, *supra* note 9 ("Albert Gidari, a telecommunications lawyer who represents several wireless providers, tells NEWSWEEK that the companies are now getting 'thousands of these requests per month,' and the amount has grown 'exponentially' over the past few years.").

12. Chief Judge Kozinski, in a dissent in which he stressed the importance of maintaining Fourth Amendment protections in the face of increasingly sophisticated forms of government surveillance, noted that "[w]hen requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use." United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing en banc).

13. *Id.* at 1125.

14. *See* Isikoff, *supra* note 9.

15. *See* discussion *infra* Sections III.A and III.B.

material to an ongoing criminal investigation,"[16] or some other "hybrid" standard—is anything but clear under current law. As various courts struggle to apply the Electronic Communications Privacy Act ("ECPA")[17] and the Fourth Amendment to compelled disclosures of location information, a messy, inconsistent legal landscape has emerged: "within the same judicial district, you might have two magistrates who disagree and issue contrary orders for the standard upon which to disclose that [location] information."[18] Indeed, the degree of confusion over the appropriate standard to apply to location information is increasing and has spread across judicial districts.[19]

The House Judiciary Committee's Subcommittee on the Constitution, Civil Rights, and Civil Liberties began to respond to this landscape of uncertainty in 2010 by holding a series of ECPA reform hearings, one of which focused specifically on location information.[20] Prior to the hearings, a

16. 18 U.S.C. § 2703(d) (2010).

17. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). This Article uses the term ECPA to describe the first three titles of the Electronic Communications Privacy Act: Title I ("Interception of Communications and Related Matters"), 100 Stat. at 1848, which amended the Wiretap Act (commonly referring to Title III ("Wiretapping and Electronic Surveillance") of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2511–2520 (2010))); Title II ("Stored Wire and Electronic Communications and Transactional Records Access"), commonly referred to as the Stored Communications Act (SCA), Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860–1868 (codified as amended at 18 U.S.C. §§ 2701–2712 (2010)); and Title III ("Pen Registers and Trap and Trace Devices"), commonly referred to as the Pen/Trap Devices statute, Pub. L. No. 99-508, tit. III, 100 Stat. 1848, 1868–1873 (codified as amended at 18 U.S.C. §§ 3121–3127 (2010)).

18. *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 26 (2010) [hereinafter *House Judiciary 2010 ECPA Reform Hearing*] (written statement of Albert Gidari, Perkins Coie LLP), *available at* http://judiciary.house.gov/hearings/printers/111th/111-98_56271.pdf.

19. *See generally ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 81–85, 93–94 (2010), [hereinafter *Location Hearing*] (written statement of Judge Stephen Wm. Smith, U.S. Magistrate Judge), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf (summarizing and collecting inconsistent decisions).

20. *See Location Hearing*, *supra* note 19. The overarching goal of this hearing was to educate Subcommittee Members about how location-based technologies and services work, and how ECPA's application to location information was creating a state of legal chaos for Magistrate Judges, as well as industry, privacy, and law enforcement stakeholders. In his opening statement at the Location Hearing, Subcommittee Chairman Jerrold Nadler remarked that:

> any legislative changes to ECPA must . . . sustain the public's confidence in the security of their communications or it [could] harm both the robust

number of companies and civil liberties groups joined together to create the Digital Due Process ("DDP") Coalition in order to propose principles to guide congressional consideration of ECPA reform.[21] One principle proposed a new standard for law enforcement access to all types of location information, stating that "[t]he Government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device."[22] This principle seeks to treat historical and prospective location information equally under the law and to require law enforcement to meet a probable cause standard before obtaining access to any location data.

Unfortunately for the privacy community, DDP's probable cause standard is a "non-starter" for law enforcement. One senior DOJ official recently told a Senate Committee that "if an amendment [to the ECPA] were to unduly restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker, or other dangerous criminal, it would have a very real and very human cost."[23] The Department of Justice will indeed resist the imposition of a high, unitary standard for location data access and will likely find no shortage of allies in Congress itself to do so effectively. Even the

> market for cell phones and the rapid innovation that is fundamental to the market's health. Because ECPA inevitably involves the interaction of all these important and complex considerations, we are taking the time through multiple hearings to educate ourselves carefully and fully before engaging in legislative action.
>
> . . .
>
> We are honored to have certain witnesses here today, who are experts in these technologies. They can give us the necessary background to embark upon an understanding of how they work, what types of information and records they can generate and store, and how they can be of assistance to law enforcement in appropriate circumstances.
>
> This initial educational effort is in my view not only warranted, but essential before we undertake any effort at amending or otherwise reforming ECPA. After we hear the terrain described, we will move on to other questions today—namely, how is ECPA currently being applied to these location based technologies and services by the courts?

Id. at 5–6.

21. *See About the Issue*, DIGITAL DUE PROCESS COALITION (May 5, 2010), http://www.digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163; *see also House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 12 (written statement of James X. Dempsey, Vice President for Pub. Policy, Ctr. for Democracy & Tech.), *available at* http://judiciary.house.gov/hearings/pdf/Dempsey100505.pdf.

22. *See Our Principles*, DIGITAL DUE PROCESS COALITION (May 5, 2010), http://www.digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163.

23. *Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 5 (statement of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice).

DDP Coalition acknowledges that ECPA reform must "preserve the 'building blocks' of criminal investigations."[24] In other words, any amendments to the ECPA must continue to enable an investigative system that allows law enforcement to compel the disclosure of various types of non-content information under lower legal standards at the early stages of an investigation. Applying these less stringent standards to non-content information avoids the premature foreclosure of valid investigations, in that it allows agents to pursue early investigative leads and "build up" to the use of more intrusive tools to obtain more sensitive information protected by higher access standards, such as the contents of communications.

But the difficulty with imposing a probable cause standard upon law enforcement access to all location data, as a matter of policy, does not minimize or negate the need for Congress to examine how law enforcement uses location information and to assess the privacy impact of current law enforcement access standards for location information. That examination will reveal an urgent need for Congress to amend the ECPA—both to clarify the law and reestablish the balance of interests among law enforcement, privacy, and industry equities.[25]

The unitary probable cause standard advocated by the privacy community and rejected by law enforcement has led to a stalemate. So, where do we find ourselves? As co-authors who approach ECPA reform from very different backgrounds and perspectives, we recognize the need to propose law enforcement standards for location information that: (1) articulate clear rules for courts to apply and law enforcement agents and industry to follow; and (2) strike a reasonable balance among the interests of law enforcement,

---

24. *Id.*; *see also House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 16–17 (written statement of James X. Dempsey). The DDP Coalition recognizes that:

> [u]nder current law, government investigators often work their way up the ladder to probable cause, starting with subpoenas for subscriber identifying information and stored transactional data, then moving to court orders under 2703(d) for more detailed transactional data and court orders, based on less than probable cause, for real-time interception of signaling and routing information. Based on analysis of this and other data, they may have probable cause to obtain a search warrant.

Id.

25. Even the Department of Justice "applaud[s] [Senate Judiciary Committee] efforts to undertake a renewed examination of whether [ECPA's] current statutory scheme . . . adequately protects privacy while at the same time fostering innovation and economic development." *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 6 (testimony of James A. Baker). Mr. Baker further notes that "[i]t is legitimate to have a discussion about our present conceptions of privacy, about judicially-supervised tools the government needs to conduct vital law enforcement and national security investigations, and how our statutes should accommodate both." *Id.*

privacy, and industry such that they could be included in legislation that might be passed by Congress. Articulating such a reasonable proposal requires knowledge of technology, law, policy, and politics.

For the purpose of offering a reasonable legislative proposal, we assume as an incontestable value that law enforcement should have access to location information that is necessary and sufficient to ensure the safety of the public by apprehending criminal perpetrators and disrupting future criminal activity—but no more. We also assume as a second and equally uncontestable value that people should be, and know they are, free from any government scrutiny of their location data that is not necessary to that public safety function. Neither of these values is an absolute one. As such, our proposal is neither the most "privacy protective" standard possible, nor the most "law enforcement friendly" standard imaginable. Indeed, what we offer in Part VI is the product of a dialogue between the authors: one a committed privacy advocate and technologist, the other a former federal prosecutor who has both used location tools in that role and considered them from a legislative perspective while working for the House Judiciary Committee.

We believe this Article will advance the debate by proposing a policy framework, including model access standards that will be palatable to all stakeholders insofar as each of their positions will be improved in some appreciable way. Part II of this Article provides a brief background discussion of various current location technologies and the level of location precision they offer. Part III explores the confusion currently plaguing courts over law enforcement access standards to location data and examines what those standards require the government to show. Part IV discusses some "lessons learned" from congressional hearings and advocacy efforts during the 111th Congress, specifically informed by Stephanie's work on the House Judiciary ECPA reform hearings. Part V examines how courts considering law enforcement access to global positioning system ("GPS") location information have articulated privacy impacts and other social harms using the interpretive frames of Orwell's dystopia in *1984*, as well as what has come to be called the "panoptic effect"—the anxious response produced by the presumed omnipresence of the government's gaze. Part V ultimately suggests that location privacy is best addressed by the legislative branch. Finally, Part VI presents a model legislative privacy framework for location information, including law enforcement access standards and other types of "downstream" privacy protections to ensure that, among other things, law enforcement agencies do not retain location data longer than needed for legitimate law enforcement purposes.

II. TECHNOLOGY

Over the past few decades, the mobile phone has evolved from a luxury status symbol to a necessity. By the end of 2010, more than ninety-five percent of the U.S. population subscribed to a mobile telephone service.[26] As consumers have embraced cellular phones, law enforcement agencies have gained access to several methods through which to obtain both historical and real-time (prospective) location information. Generally speaking, this information can be separated into two categories: passive collection of information incident to the delivery of cellular services, and active surveillance in which information is collected and processed solely to benefit law enforcement agencies. In addition to this distinction, there are several different technologies that can be used to obtain location information—some highly accurate, others much less so, but with the general direction of innovation tending towards greater precision. The purpose of this Part is to provide the reader with a brief introduction to each of these technologies and the ways in which they can be used to determine or track the location of individuals.

A. A BRIEF INTRODUCTION TO CELL PHONE TECHNOLOGY

Unlike conventional "wireline" phones, mobile phones use radio to communicate between the customer's telephone and the carrier's network. Service providers maintain large numbers of radio base stations (also called "cell sites") spread throughout their geographic coverage areas.[27] These cell sites are generally located on "cell towers" serving geographic areas of varying sizes, depending upon topography and population concentration. Service providers are deploying higher-capacity network architectures, with the potential to provide more precise information regarding a phone user's location.

As part of their normal function, mobile phones periodically identify themselves to the nearest cell site as they move about the coverage area.[28]

---

26. *Wireless Quick Facts*, CTIA—WIRELESS ASS'N (2011), http://www.ctia.org/advocacy/research/index.cfm/aid/10323.

27. Press Release, Informa Telecoms & Media, The Shape of Mobile Networks Starts To Change as Femtocells Outnumber Macrocells in US (Oct. 21, 2010), http://femtoforum.org/fema/pressreleases.php?id=269 ("[F]emtocells now outnumber conventional outdoor cell sites in the United States marking a major milestone in the evolution of mobile networks. Conservative estimates suggest there are currently 350,000 femtocells and around 256,000 macrocells in the US. Furthermore by March 2011, there are expected to be at least twice as many femtocells as macrocells in the US.").

28. *Location Hearing*, *supra* note 19, at 13 (testimony of Prof. Matt Blaze, Univ. of Pa.) ("Cell phones, as they move and as they are turned on, discover the base station with the

This enables wireless carriers to know how to reach a particular subscriber's phone when it receives a call. Of course, mobile telephones (as their name suggests) are portable, and so when a phone moves away from the cell site with which it started a call and nearer to a different cell site, the call is "handed over" from one cell site to another without interruption.[29]

Each cell site has a large but fixed maximum capacity that can transmit a limited number of concurrent calls and data streams. In an area with a low number of users (or users who make few calls and who are not heavy users of data services), only a few cell sites will be necessary, and each can serve a large geographical area. In areas with large numbers of active users, however, and particularly those who make heavy use of data services, a carrier will need to place far more cell sites, each serving a smaller geographic area, to compensate for the relatively larger usage burden placed on the local network.[30] Carriers that do not or cannot deploy more cell sites to cope with increased demand suffer from slow data speeds and frequent dropped calls.[31] As such, rural areas tend to have fewer cell sites, each with greater service areas, than urban areas, which generally have far more sites that are spaced closer together. Obviously, the proximity of one cell site to another in a geographic area is one factor in the production of more accurate location data.

---

strongest radio signal and perform a registration process identifying themselves, establishing that the user has a valid cell phone service, and identifying the local base station that is best equipped to process the call by virtue of the strength of its radio signal."); *see also id.* at 20 (written statement of Prof. Matt Blaze).

29. *Id. See generally* Nishith D. Tripathi, Jeffrey H. Reed & Hugh F. VanLandingham, *Handoff in Cellular Systems*, IEEE PERS. COMM., Dec. 1998, at 26, *available at* http://www.scss.tcd.ie/Hitesh.Tewari/papers/tripathi98.pdf.

30. *Location Hearing*, *supra* note 19, at 15 (testimony of Prof. Matt Blaze) ("[T]oday the limiting factor in how far apart [cell sites] can be is the number of customers they have to serve. And as this technology has exploded, the number of customers in any given area has gone explosively up, particularly in urban and densely populated areas.").

31. For example, one carrier has a reputation for dropped calls in some urban areas like San Francisco, due to the presence of large numbers of tech-savvy users with data-hungry iPhones, combined with the three-year waiting time required by the local authorities to get permission to erect new cell towers (which is often combined with further local obstructionism, whether motivated by opportunistic financial holdups or by NIMBY reactions to cell tower construction from individuals and communities with valuable real estate holdings). *See* Edward Wyatt, *AT&T and T-Mobile Chiefs Field Skeptical Questions on Capitol Hill*, N.Y. TIMES (May 11, 2011), http://www.nytimes.com/2011/05/12/technology/12phone.html ("T-Mobile ads made merciless fun of AT&T's reputation for dropped calls and sluggish wireless data connections"); MG Siegler, *Steve Jobs Continues To Answer the Questions That AT&T Won't*, TECHCRUNCH (July 18, 2010), http://techcrunch.com/2010/07/18/steve-jobs-att-2/ ("[Apple CEO Steve Jobs] said that it takes [AT&T] three years to get approval for a new cell tower in San Francisco. Yes, three years. '*That's the single biggest problem they're having*,' Jobs said. . . . Jobs also noted at the press conference that it takes '*about three weeks*' to add a new cell tower in Texas.").

B. CELL SITE DATA

Wireless service providers retain detailed logs for diagnostic, billing, and other purposes. These logs reveal the calls and Internet connections made and received by wireless subscribers, as well as detailed technical information regarding the cell sites that were used.[32] Such logs generally only reveal which particular cell site a phone was near at the time of the call.

Data from multiple towers can be combined to pinpoint (or "triangulate") a phone's latitude and longitude with a high degree of accuracy (typically under fifty meters).[33] This triangulated cell site data is generally only available prospectively, either due to a 911 call by a subscriber, or because a law enforcement agency has asked a carrier to collect it. Some carriers do routinely track and record triangulated data, and movement toward this practice is a general trend in the industry, although it is not yet the dominant practice, much less the common policy of all companies.[34] As such, law enforcement agencies can also obtain high-accuracy, triangulated historical data when it is available due to a specific company's data collection practices.

C. GLOBAL POSITIONING SYSTEM ("GPS")

Many mobile phones now include special hardware that enables the device to receive signals from a constellation of global position satellites.[35] Software on the phone can use these signals to calculate latitude and longitude,

32. McCullagh, *supra* note 2 ("Cellular providers tend not to retain moment-by-moment logs of when each mobile device contacts the tower, in part because there's no business reason to store the data, and in part because the storage costs would be prohibitive. They do, however, keep records of what tower is in use when a call is initiated or answered . . . ."); *see also* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, RETENTION PERIODS OF MAJOR CELLULAR SERVICE PROVIDERS (2010), *available at* http://www.wired.com/images_blogs/threatlevel/2011/09/retentionpolicy.pdf (listing, in chart form, data retention periods by the major cellphone carriers).

33. This requires the placement of special radio equipment at each cell site. *See generally Location Hearing*, *supra* note 19, at 38–41 (statement of Michael Amarosa, Sr. Vice President for Public Affairs, TruePosition Inc.).

34. *Location Hearing*, *supra* note 19, at 26–27 (written statement of Prof. Matt Blaze) ("(Whether locations are routinely tracked and recorded at times other than when calls are made or received depends on the policy of the particular carrier.) . . . Some carriers also store frequently updated, highly precise, location information not just when calls are made or received, but about every device as it moves about the networks. Maintaining such detailed records about the locations of phones as they move from place to place makes good engineering sense, and we should expect this trend to continue as part of the natural progression of technology.").

35. This communication is one-way. Phones receive signals from the satellites but do not transmit anything back to them.

often with a high degree of accuracy (less than twenty-five meters).[36] Although GPS is often more accurate than any other location technology, there are a few limitations: GPS signals are weak, high-frequency signals that do not penetrate walls, and as a result GPS often does not work when indoors. Moreover, for the same reason, GPS often does not function well in "urban canyons" due to signal deflection off of the sides of tall buildings. Furthermore, the GPS functionality tends to use significant amounts of power, which can lead to shorter battery life.[37] When GPS functionality is available, wireless carriers can prospectively obtain a device's location, such as when the user dials 911, or when asked to do so by law enforcement agencies. Carriers do not generally have historical GPS data to deliver.

Many smartphones now provide access to the GPS functionality to third-party "apps" installed on the devices. As such, app developers and location service providers also have access to users' GPS location data, often far more than the wireless carriers, although this is usually with the user's knowledge and consent.[38] Law enforcement agencies can compel these location service providers to disclose the historical GPS data in their possession, although prospective disclosures are limited to user-initiated "check-ins," as these companies are usually not able to generate their own GPS queries.

D. WIFI

Many smartphones include wireless internet ("WiFi") functionality, enabling device owners to browse the web at much faster speeds (and without impacting their carrier-imposed data cap) when at home, work, or in many public places. In addition to providing a connection to the Internet, the WiFi connections can also be used to determine the approximate location of the device.

---

36. *Location Hearing*, *supra* note 19, at 55 (attachment to written statement of Michael Amarosa).

37. Letter from Andy Lees, President, Mobile Commc'ns Bus., Microsoft Corp., to Rep. Fred Upton et al. (May 9, 2011), *available at* http://blogs.technet.com/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-82-95/2451.Consumer-Privacy-_2600_-Windows-Phone-7-_2D00_Submission-to-House-Energy-and-Commerce-Committee-_2D00_-5.9.2011.pdf ("Windows Phone 7 generally relies upon WiFi access point or cell tower information to determine a phone's approximate location because GPS location data is not always available, and when it is, it can draw more heavily on battery power . . . .").

38. If a user "checks in" with a location provider like Foursquare, that location provider will learn their location, but the wireless carrier will not, as the information is sent directly to the location provider.

Several companies have created databases listing wireless networks and their approximate geographic location.[39] Initially, these databases were populated with data obtained by driving through the streets of cities around the world, collecting the data with a laptop or other special hardware.[40] In recent years, however, Google, Apple, and Microsoft have all enlisted the "crowdsourced" assistance of millions of smartphones to collect this data for them.[41]

By determining the available WiFi networks and submitting this list to one of the database providers, applications on the device and the platform mobile vendor (e.g., Google, Apple) can quickly determine the user's approximate location without using GPS, which would consume significantly more battery power.[42] Location data is increasingly valuable, enough so that the major platform vendors have been "willing to push the envelope on privacy to collect it."[43] Not only is location data used for maps and

39. *See* Greg Stirling, *Google Ends Street View WiFi Data Collection, May Now Need Other Sources for Location*, SEARCH ENGINE LAND (Oct. 20, 2010), http://searchengineland.com/google-ends-street-view-wifi-data-collection-potentially-needs-other-sources-for-location-53373 ("One of the purposes of collecting WiFi locations is to enable Google to identify user location (on handsets, laptops and PCs to some degree) through triangulation using a database of hotspots."); *see also Frequently Asked Questions*, SKYHOOK WIRELESS, http://www.skyhookwireless.com/howitworks/faq.php (last visited Mar. 17, 2012) ("Skyhook deploys vehicle-based signal scanning and data collection technologies, a common practice in the digital mapping and data collection industries. These Skyhook-equipped vehicles conduct systematic and comprehensive signal surveys by traveling every public road and highway in targeted coverage areas. These signal surveys capture the data output of individual access points and pair them with a date, time, and location stamp at the point where they are received by the data collection device.").

40. *See* Brad Stone, *Google Says It Collected Private Data by Mistake*, N.Y. TIMES (May 14, 2010), http://www.nytimes.com/2010/05/15/business/15google.html ("[B]ecause of a programming error in 2006, the company had . . . been mistakenly collecting snippets of data that happened to be transmitted over non-password protected wi-fi networks that the Google camera cars were passing."); *see also* Jenna Wortham, *Cellphone Locator System Needs No Satellite*, N.Y. TIMES (May 31, 2009), *available at* http://www.nytimes.com/2009/06/01/technology/start-ups/01locate.html (explaining how the company Skyhook "uses the chaotic patchwork of the world's wi-fi networks, as well as cell towers, as the basis for a location lookup service").

41. Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, WALL ST. J. (Apr. 22, 2011), http://on.wsj.com/zp2Euo ("Apple Inc.'s iPhones and Google Inc.'s Android smartphones regularly transmit their locations back to Apple and Google, respectively . . . as part of their race to build massive databases capable of pinpointing people's locations via their cell phones.").

42. *See generally* John Morris, *Apple Trades Privacy for Battery Life, Instead of Protecting Both*, CENTER FOR DEMOCRACY & TECH. (Apr. 22, 2011), https://www.cdt.org/blogs/john-morris/apple-trades-privacy-battery-life-instead-protecting-both.

43. Miguel Helft, *Apple and Google Use Phone Data To Map the World*, N.Y. TIMES (Apr. 25, 2011), https://www.nytimes.com/2011/04/26/technology/26locate.html.

navigation services on mobile devices, but it is also used to customize advertising aimed at people in a particular place. Such ads are far more lucrative than other ads and are becoming a major portion of the mobile advertising market, which industry experts estimate will be a $2.5 billion market by 2015.[44] Not only do these economic factors encourage companies to collect more location data, but they also encourage the collection of data with greater accuracy, allowing merchants to pitch advertisements to consumers walking past their store, rather than just those in the neighborhood.

E. PINGS

Most of the location information described in this Part is collected in the process of providing wireless voice and data services, or due to users calling 911 or using a location-enabled app on their smartphones. For such information, law enforcement agencies can either request historical data already stored by the provider, or request prospective surveillance that will provide data to the law enforcement agency as soon as the carrier receives it. In either case, the information collection is passive, in that no new data is generated due to the law enforcement surveillance request.

It is also possible, however, for carriers to monitor their customers actively, generating new data specifically in response to a request from law enforcement agencies. In such scenarios, the wireless carriers can covertly "ping" a subscriber's phone in order to locate them when a call is not being made. Such pings can merely reveal the nearest cell site to the subscriber,[45] or more accurate GPS or triangulated data if requested.[46] In addition to the

---

44. *Id.*

45. *See* Stone v. State, 941 A.2d 1238, 1244 (Md. Ct. Spec. App. 2008) ("Trooper Bachtell obtained the appellant's cell phone number and contacted his cell phone service provider. At Trooper Bachtell's request, the service provider conducted a 'ping' of the appellant's cell phone, which revealed that the phone was 'within a two mile radius of the Frederick County Detention Center.' ").

46. *See* Comments of CTIA—The Wireless Association on U.S. Department of Justice Petition for Expedited Rulemaking at 17, *In re* Petition for Expedited Rulemaking To Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcemenet Act, Docket No. RM-11376 (Fed. Commc'ns Comm'n July 25, 2007), *available at* http://fjallfoss.fcc.gov/ecfs/comment/view?id=5514711157 ("Law enforcement routinely now requests carriers to continuously 'ping' wireless devices of suspects to locate them when a call is not being made . . . so law enforcement can triangulate the precise location of a device and [seek] the location of all associates communicating with a target."); *see also* Devega v. State, 689 S.E.2d 293, 299 (Ga. 2010) ("[T]he investigators requested that Devega's cell phone provider 'ping' his phone, which the officers described as sending a signal to the phone to locate it by its global positioning system (GPS). The company complied and informed the police that the phone was moving north on Cobb Parkway.").

carrier-initiated pings, law enforcement agencies have also performed "low tech" pings by calling a target and hanging up before the phone rang, in order to generate cell site data that could then be requested from the carriers.[47]

F. TRENDS

The increasing accuracy and use of location data is motivated by the proliferation and advancement of mobile technology, as well as the lucrative commercial market for location-based services and marketing. Within that general context, there are several trends worth noting that suggest that single cell site data will become increasingly accurate. This postulation is particularly significant for evaluating current DOJ policies governing the legal standards for law enforcement's compelled disclosures of prospective location information.[48]

First, in an attempt to "fill the gaps" in their coverage, wireless carriers have, in the past few years, distributed hundreds of thousands of "microcells," "picocells," and "femtocells" to customers, which connect to the user's broadband internet connection and provide cellular connectivity to phones within tens or hundreds of meters. Industry estimates indicate that there are already more than 350,000 femtocells deployed in the United States, as compared to the more than 250,000 traditional carrier cell sites.[49] As these devices often broadcast a signal no further than a subscriber's home, the accuracy of single cell site location data can in some cases be more accurate than GPS, depending on whether the target is connected to a traditional cell site, or a residential femtocell.

Second, the success of Apple's iPhone and other smartphones has led to a massive increase in the use of data by mobile users. For example, AT&T has seen an 8,000 percent increase in data traffic between 2007 and 2010.[50] In response to this increased demand on their networks, carriers are deploying new cell sites and reducing the coverage area of existing towers.[51] As carriers

47. United States v. Forest, 355 F.3d 942, 947 (6th Cir. 2004) ("In order to reestablish visual contact, a DEA agent dialed Garner's cellular phone (without allowing it to ring) several times that day and used Sprint's computer data to determine which cellular transmission towers were being 'hit' by Garner's phone. This 'cell site data' revealed the general location of Garner.").

48. *See infra* Section III.A.1.

49. Press Release, Informa Telecoms & Media, *supra* note 27.

50. Dan Meyer, *AT&T Filing Provides Interesting Industry Data*, RCR WIRELESS (Apr. 25, 2011), http://www.rcrwireless.com/article/20110425/CARRIERS/110429949/att-filing-provides-interesting-industry-data.

51. Tracy Ford, *Tower Industry Primed for Growth with Carrier Buildouts*, RCR WIRELESS NEWS (Mar. 3, 2010), http://www.rcrwireless.com/ARTICLE/20100303/INFRASTRUCTURE/100309979/tower-industry-primed-for-growth-with-carrier-buildouts ("LTE

embrace faster 4G mobile data technologies, they will need even more cell sites, further reducing the coverage area around each tower.

As the coverage area around each traditional cell tower shrinks, and consumers increasingly embrace femtocells in their homes and businesses, single cell site data will become far more accurate—in some cases as good as GPS, and in others pinpointing someone's location to an area the size of a few blocks.

III. THE LAW

This Article proposes a policy framework that balances the interests of stakeholders affected by law enforcement access standards for provider-held location information. Before turning to policy proposals, the Article first discusses how law enforcement currently justifies its collection of prospective and historical location data—both under the DOJ's current interpretation of the law and the suggested policy guidance it gives to prosecutors and agents in the field.

This Part describes how the DOJ's and courts' various statutory interpretations have created a set of conflicting standards for law enforcement access to location data. Changes in technology, combined with the instability in the law created by conflicting legal standards for location data, create a critical need for Congress to amend the law to produce a better balance among privacy, law enforcement, and industry equities—a balance that would ideally benefit all stakeholders in some appreciable way. As such, this Part seeks to identify where that balance, as a matter of policy, may lie and how new law enforcement access standards or other "downstream" privacy protections might serve that legislative end. This Part therefore focuses on the policy implications of the current law, not on how the Fourth Amendment might apply to law enforcement access to location data held by a third party. When and under what circumstances the Fourth Amendment might require law enforcement to obtain a warrant to obtain location information from third-party providers remains a contested area of the law[52] and one that is

is going to be driving revenue for the tower companies . . . as a result of the incredible demand supported by LTE 700 MHz spectrum and the resulting splitting and additional coverage and capacity that the carriers are going to have to put in place to meet that demand.").

52. *Compare* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 677, 717 (2011) (arguing that courts should require a warrant for access to location data in all cases because such acquisition is a search under the Fourth Amendment), *with* Orin S. Kerr, *Court Rules That Police Cannot Use Warrants To Obtain Cell Phone Location of Person Who Is Subject of Arrest Warrant*, VOLOKH CONSPIRACY (Aug. 8, 2011), http://volokh.com/2011/08/08/court-rules-that-police-cannot-use-warrants-to-obtain-cell-phone-location-of-person-who-is-subject-of-arrest-warrant/ (arguing that location

beyond the scope of this Article to reconcile. To the extent that the discussion touches upon Fourth Amendment issues, it does so in the service of describing and developing a policy discussion, not to offer an opinion on the correct application of the Fourth Amendment to location information.

A. LEGAL BACKGROUND FOR REAL-TIME OR "PROSPECTIVE" CELL SITE DATA

Locating the proper law enforcement access standard for prospective location data in the current law is, in some respects, like the quest for the Holy Grail, the search for the fountain of youth, or the hunt for a truly comfortable pair of high heels—one is unlikely to find them. This legal mystery remains unsolved primarily for two reasons. First, the ECPA[53]—the primary law governing law enforcement access to wire, oral, and electronic communications and other stored subscriber records and information—does not contain the word "location" in any part of the statute or otherwise provide language that could be easily interpreted to cover law enforcement access to real-time location data from third-party providers.[54] Second, Congress, in a different statute, has only expressed what is *insufficient* for purposes of law enforcement access to prospective location information from a third-party provider, but not what is either *necessary* or *sufficient* for such compelled disclosures. Indeed, the Communications Assistance for Law Enforcement Act ("CALEA") merely instructs that "any information that may disclose the physical location of [a telephone service] subscriber" may

information of phones is not protected by the Fourth Amendment under *Smith v. Maryland*, 442 U.S. 735 (1979)).

53. *See supra* note 17.

54. Consider, for example, the testimony of Judge Smith describing the difficulty he and other Magistrate Judges have faced in determining the proper law enforcement access standard for real-time location information:

> Moreover, none of the other categories of electronic surveillance seemed to fit. The pen register standard was ruled out by a proviso in a 1994 statute known as CALEA. The wiretap standard did not apply because CSI does not reveal the contents of a communication. The Stored Communications Act (SCA) standard did not seem to apply for two reasons: the definition of "electronic communication" specifically excludes information from a tracking device; and the structure of the SCA was inherently retrospective, allowing access to documents and records already created, as opposed to prospective real time monitoring.

Location Hearing, *supra* note 19, at 82–83 (footnotes omitted); *see also* Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 606–09 (2007) (analyzing how the Wiretap Act and Pen/Trap statute do not provide the requisite authority for such "tracking" and the SCA only authorizes retrospective access to previously stored communications content and non-content information).

not be acquired "solely pursuant to the authority for pen registers and trap and trace devices."[55] Therefore, with respect to a compelled disclosure, if real-time location data cannot be provided to law enforcement "*solely pursuant*" to a court order for a Pen/Trap device, there must be some further requirement. But that requirement, unfortunately, remains undefined in the law. This exercise in *Via Negativa*[56] makes for great scholastic discussions about the incomprehensible character of an ineffable God but it is not very effective as a descriptive tool for discerning a legal standard. At best, it is a rather ineffective inversion of Justice Stewart's famous concurrence in *Jacobellis v. Ohio* about the similar difficulty the Court encountered in defining "hard core pornography" with any accuracy: "I know it when I [don't] see it."[57] Stated more precisely, if less concisely and memorably, "I'll know it when I can infer its existence and nature by seeing everything that it is not."

1. The DOJ's Interpretation of the Standard for Obtaining Prospective Cell Site Data

Lacking clear, affirmative statutory guidance, the DOJ has routinely acquired, since at least 2005, certain categories of "less precise" prospective cell site information through the *combination*[58] of two court orders: (1) a Pen/Trap court order pursuant to 18 U.S.C. § 3123,[59] and (2) a "D" Order pursuant to 18 U.S.C. § 2703(d), a section of the Stored Communications Act ("SCA") that permits the government to compel the production of non-

55. 47 U.S.C. § 1002(a)(2) (2010).

56. The "Via Negativa" is a method of philosophical and theological argument often associated with mysticism, sometimes referred to as "negative" or "apophatic" theology that attempts to describe God or the divine good by negation, specifically in terms of what God is *not* (*apophasis*), discerning instead only what may not be said accurately concerning the goodness and perfection(s) of God, which are beyond direct expression. The technique has its roots in several Greek philosophical schools, as well as several Western and Eastern religious traditions. *See Negative Theology*, THE BLACKWELL DICTIONARY OF WESTERN PHILOSOPHY 465–66 (Nicholas Bunnin & Jiyuan Yu eds., 2004); *see also* KAREN ARMSTRONG, THE CASE FOR GOD 317 (2009) (describing the potential resurgence of apophatic argument in postmodern theology).

57. Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

58. *See* Bankston, *supra* note 54, at 609–12 (describing the first publically known case where the DOJ articulated the "hybrid theory" in applying for a court order authorizing access to real-time cell site information).

59. 18 U.S.C. § 3123(a)(1) (directing that a court "shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device . . . if the court finds that the attorney for the Government [in an application pursuant to 18 U.S.C. § 3122(a)(1)] has certified to the court that the information likely to be obtained . . . is relevant to an ongoing criminal investigation").

content records or information pertaining to a subscriber or customer.[60] When combined, these two orders are known as a "hybrid order."[61] A DOJ manual documents that the rationale behind the DOJ's "hybrid" use of these two statutes derives from a combination of discrete statutory requisites.[62] First, because "cell-site data is 'dialing, routing, addressing or signaling information,' . . . 18 U.S.C. § 3121(a) requires the government to obtain a Pen/Trap order to acquire this type of information."[63] Second, however, because CALEA "precludes the government from relying 'solely' on the authority of the Pen/Trap statute to obtain cell-site data for a cell phone . . . some additional authority is required to obtain prospective cell-site information."[64] The DOJ asserts that "[s]ection 2703(d) provides this authority because . . . it authorizes the government to use a court order to obtain all non-content information pertaining to a customer or subscriber of an electronic communications service [or a remote computing service]."[65]

The same DOJ manual, published in its third edition in 2009, also provides guidance about the "precision" of the information likely to be obtained from cell site data (exclusive of GPS location technologies). The manual instructs that "[c]ell-site data identifies the antenna tower and, in some cases, the 120-degree face of the tower to which a cell phone is connected, both at the beginning and the end of each call made or received by a cell phone."[66] The manual further explains that "[t]he towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more

60. *See id.* § 2703(c) (authorizing law enforcement to compel "a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the government entity . . . obtains a court order for disclosure under subsection (d) of this section . . .").

61. U.S. DEP'T OF JUSTICE (DOJ), SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 160 (3d ed. 2009) [hereinafter DOJ MANUAL], *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

62. *Id.* at 159–60. Some published decisions also indicate that DOJ prosecutors have, at times, offered the All Writs Act, ch. 646, § 1651, 62 Stat. 869, 944 (codified as amended at 28 U.S.C. § 1651 (2010)), as a "mechanism for the judiciary to give [the government] the investigative tools that Congress has not." *In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device (*In re E.D.N.Y. Application*), 396 F. Supp. 2d 294, 325 (E.D.N.Y 2005); *see also In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register (*In re W.D.N.Y. Application*), 415 F. Supp. 2d 211, 219 (W.D.N.Y 2006). These courts did not endorse this theory.

63. DOJ MANUAL, *supra* note 61, at 159–60.

64. *Id.* at 160.

65. *Id.*

66. *Id.* at 159.

apart even in urban areas."[67] Relying on this description of cell tower technology, the manual concludes: "[A]t best, these data reveal the neighborhood in which a cell phone user is located at the time a call starts and at the time it terminates; it does not provide continuous tracking and is not a virtual map of a cell phone user's movements."[68]

This description of the relative precision of cell site data, even if it is intended only to apply to single cell tower data (i.e., no multi-tower, triangulation, or GPS location information), will soon be—if it is not already—outdated with the deployment of microcell, picocell, and femtocell technology that, in some cases, can be more accurate than GPS.[69] Indeed, in urban areas and other environments where microcell technology is present, a cell phone's location can be identified on an individual floor or room within a building.[70] Moreover, the precision of single cell tower data will only increase as providers deploy new cell sites to cope with the surge in mobile user data traffic.[71]

The DOJ manual further advises prosecutors that *in most districts* they may obtain prospective cell site information with the use of hybrid orders, but it also acknowledges that some magistrate judges require a "probable cause" showing before authorizing law enforcement access to any type of prospective cell site data.[72] This split among magistrate judges, characterized by one federal prosecutor as the "Santa Ana Judicial Revolt,"[73] is discussed next.

2. *Judicial Resistance to the Government's Use of Hybrid Orders*

A growing number of magistrate judges within and across various judicial districts have rejected the government's use of the hybrid theory to obtain any type of prospective cell site information.[74] Some courts have held that, as

67. *Id.* (citing *In re* Application of the United States of America for an Order for Disclosure of Telecomm. Records and Authorizing the Use of a Pen Register and Trap and Trace (*In re S.D.N.Y. Application*), 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005)).

68. *Id.*

69. *See Location Hearing*, *supra* note 19, at 25 (written statement of Prof. Matt Blaze, Univ. of Pa.).

70. *Id.*

71. *Id.*

72. DOJ MANUAL, *supra* note 61, at 159–60.

73. E-mail from Tracy Wilkison re: Changes to GPS / Cell Site for Investigations Form (July 28, 2008) (informing other prosecutors about changes in office procedures for obtaining GPS and cell site information), *in* U.S. Dep't of Justice, Response to Freedom of Information Act Request No. 07-4123 re: Mobile Phone Tracking 13 (Sept. 8, 2008), *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_074123_20080911.pdf.

74. *Location Hearing*, *supra* note 19, at 81–85, 93–94 (testimony of Judge Stephen Wm. Smith, U.S. Magistrate Judge). FED. R. CRIM. P. 41(d)(1) directs that "after receiving an

a matter of statutory construction, the Pen/Trap order and the D Order cannot be used to obtain prospective cell site information, but that Rule 41 provides the necessary authority because "it governs any matter in which the government seeks judicial authorization to engage in certain investigative activities."[75] More specifically, some of these courts have found that compelled disclosure of prospective cell site data is more akin to a tracking device placed under a vehicle, as defined in 18 U.S.C. § 3117,[76] than to the combination of elements comprising the government's hybrid theory and, therefore, would prompt the prudent prosecutor to obtain a Rule 41 warrant.[77]

Even the magistrate and district judges that have accepted hybrid orders and issued published decisions on the question have restricted law enforcement access to limited cell site information "yielding only generalized location data."[78] Magistrate Judge Gorenstein from the Southern District of New York, in what may be the "most cogent expression"[79] by a court in accepting the government's hybrid theory, specifically noted:

> [The government's request pertained to cell site information] tied only to telephone calls actually made or received by the telephone user . . . [with] no data provided as to the location of the cell phone when no call is in progress. [And], at any given moment, data is provided only as to a single cell tower with which the cell phone is communicating. Thus, no data is provided that could be "triangulated" to permit the precise location of the cell phone user.[80]

affidavit or other information," a judge "must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device."

75. *In re E.D.N.Y. Application*, 396 F. Supp. 2d 294, 322 (E.D.N.Y 2005); *see also In re W.D.N.Y. Application*, 415 F. Supp. 2d 211, 219 (W.D.N.Y 2005) ("[T]he challenge here is to the *statutory* justification for . . . [the government's] application. . . . The Court does not agree with the government that it should impute to Congress the intent to 'converge' the provisions of the Pen Statute, the SCA, and CALEA to create a vehicle for disclosure of prospective cell information on a real time basis on less than probable cause.").

76. "As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b) (2010).

77. *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority (*In re 2005 S.D. Tex. Application*), 396 F. Supp. 2d 747, 753–64 (S.D. Tex. 2005); *In re E.D.N.Y. Application*, 396 F. Supp. 2d at 322.

78. *Location Hearing*, *supra* note 19, at 93–94 (Exhibit B to written statement of Judge Stephen Wm. Smith) (collecting Magistrate and District Court published decisions where courts have accepted hybrid orders for limited cell site data pertaining to single cell tower and call-related information).

79. *Id.* at 83.

80. *In re S.D.N.Y. Application*, 405 F. Supp. 2d 435, 437–48 (S.D.N.Y 2005). Judge Gorenstein notes differences between the instant case and three published decisions denying

Judge Gorenstein further explained that his analysis for the instant Order was based on the "technology that is available to the Government in the District," recognizing that, with respect to future cases, "[he could not] know how . . . technology may change."[81]

For Judge Gorenstein, then, the current capacity of the cell tower network in question (the court even looked at a map of the location of various cell towers in lower Manhattan—an area it described as "densely populated by cell towers")[82] was a factor in authorizing law enforcement access to the cell site data with a hybrid order.[83] If that network's capabilities were to change due to an evolution in technology that yielded more precise location information, the court might rule differently in future cases. Indeed, the court's order might be as ephemeral as the capacities of the specific network the opinion seeks to comprehend at a specific moment in time. Any upgrade to that network that would enhance the accuracy of its geolocation capabilities in the district, made any time after the signing of the opinion, tied as it is to the facts describing the network's capacities, could render that opinion legally moot.

3. Divergent Interpretations of the Standard for Requiring Disclosure of Prospective Cell Site Data Create Legal Uncertainty

When seeking to compel "more precise" prospective location data generated by GPS or similar technologies, the DOJ's policy is to obtain a warrant based on probable cause.[84] While privacy advocates might view this as a small concession by the government, it is at best a transient one, since a policy decision by the DOJ is by no means a permanent or legally binding

government access to cell site information with a hybrid order insofar as "[t]hese cases appear to involve requests for cell site information that go beyond both what has been sought in this case and what has actually been received by the Government pursuant to any cell site application in this District." *Id.* (citing *In re 2005 S.D. Tex. Application*, 396 F. Supp. 2d 747; *In re E.D.N.Y. Application*, 396 F. Supp. 2d 294; *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Caller Identification Sys. on Tel. Numbers [Sealed], 402 F. Supp. 2d 597 (D. Md. 2005)).

81. *In re S.D.N.Y. Application*, 405 F. Supp. 2d at 450.

82. *Id.* at 437.

83. *See also In re* Application of U.S. for an Order, 411 F. Supp. 2d 678, 680–82 (W.D. La. 2006) (granting an application for cell site information consistent with Judge Gorenstein's reasoning and scope of production of cell site information, recognizing that Judge Gorenstein "limit[ed] his opinion to the particular application before him" and characterizing the single cell site technology of that time as "not permit[ting] detailed tracking of a cell phone user within any residence or building").

84. *Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 7 (testimony of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice).

decision.[85] To the extent that this policy decision protects privacy, it can be so unstable as to be subject to changes in leadership at various levels, even within a single administration, whose individual decisions implement the enforcement and oversight of a particular policy across various field offices.[86]

More troubling from a systemic perspective, however, is the inconsistent legal landscape that conflicting magistrate and district court decisions create across the country, sometimes even within the same district.[87] The system neither serves law enforcement needs nor protects privacy interests when legal standards are so uncertain. Moreover, as Judge Gorenstein's opinion illustrates, such uncertainty is magnified into legal instability, potentially to the point of unreliability, when a court's analysis is so tied to the state of

85. A DOJ policy decision, such as a policy requiring a warrant for law enforcement to acquire GPS-generated location data, has no binding authority on state or local law enforcement practices, and state investigators do not always follow DOJ policies. For example, in *Devega v. State*, investigators, without a warrant, requested a defendant's cell phone provider to "ping" his phone, which involved sending a signal to locate it through GPS information. 689 S.E.2d 293, 299 (Ga. 2010).

86. Consider, for example, Magistrate Judge Feldman's exchange with an Assistant United States Attorney ("AUSA") at oral argument. *See In re W.D.N.Y. Application*, 415 F. Supp. 2d 211, 218 (W.D.N.Y. 2006). While the government was only seeking "general [prospective cell site] location information" in the instant case, the AUSA conceded that in previous "hybrid" applications, the government had sought "prospective cell site data that could be used by law enforcement to triangulate the location of a cell phone to a degree perhaps beyond 'general location information.' " *Id.* The court pressed government counsel regarding whether the position that a hybrid order was appropriate for anything other than "general location information" had been abandoned. The AUSA responded:

> Well there's a couple of practical things going on. One, we're before magistrate judges that are the gatekeepers—we're trying to convince them that the government isn't being some ruthless, overbearing entity—we're trying to be reasonable. So, therefore, if we can get the magistrate's ear and we don't have to fight this fight a zillion times, we'll back off. If you have this internal radar that's going "privacy interest, privacy interest", okay we'll back off. But is it possible the argument could be made that we could be here on another day having gotten to floor one and now we're trying to get to floor two? Yes. Has that been suggested by anyone? Absolutely not.

Id. at 218 n.5; *see also* Freiwald, *supra* note 52, at 717 (discussing one U.S. Attorney's Office's failure to comply with DOJ policy advising agents to establish probable cause when seeking location data indicating a target's latitude and longitude (using either GPS or similarly precise data)).

87. *See Location Hearing*, *supra* note 19, at 83–85, 93–94 (written statement of Judge Stephen Wm. Smith and Exhibit B thereto). *Compare In re* an Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06 CRIM. MISC. 01, 2006 WL 468300 (S.D.N.Y. 2006) (denying application for limited single tower data), *with In re S.D.N.Y. Application*, 405 F. Supp. 2d 435 (granting application for limited single tower data).

technology in a particular district at a particular moment in time that it hinges upon a court's own examination of a network map of cell towers in a particular district—which would now include microcells, picocells, and femtocells—combined with expert opinion on the accuracy of location data that network could produce.[88] The court analyzed and accepted the government's hybrid theory (while, at the same time, limiting its ruling to the state of the technology available to the government in the district at that time), but it declared the result "unsatisfying" given Congress's lack of clear guidance regarding the appropriate standard for law enforcement access to prospective cell site data.[89]

Even the DOJ has acknowledged the need for legislation to clarify the standard governing compelled disclosures of prospective cell site data. The DOJ, however, carefully limited its recommendation to "cell tower information associated with cell phone calls," which is perhaps the particular area where the DOJ seeks specifically to retain the more nimble and efficient investigative standard provided by the hybrid order,[90] as opposed to the higher probable cause standard.[91] In the DOJ's view, "[s]ome courts . . . have conflated cell site location information with more precise GPS (or similar) location information"[92] and, as previously noted, they are already advising prosecutors to seek probable cause warrants for "more precise" GPS location data.

With location information—including single cell tower data—becoming only more precise over time and courts continuing to search for an illusory "intended" congressional standard to govern law enforcement access to prospective location data, the search for clarity remains an uncertain one at best in the absence of congressional action.

B. LEGAL BACKGROUND FOR HISTORICAL CELL SITE DATA

If the uncertainty over what standard to apply to prospective location information has left courts without a strong sense of direction, that

88. *See In re W.D.N.Y. Application*, 415 F. Supp. 2d at 213 n.3 (reviewing a letter from Verizon's Court Order Compliance Manager "which states that the information sought will only 'identify the general area that the target mobile phone located at the time of a specific call' and that it 'cannot pinpoint the exact location of the mobile phone' ").

89. *In re S.D.N.Y. Application*, 405 F. Supp. 2d at 442.

90. *Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 5 (testimony of James A. Baker).

91. Mr. Baker explains earlier in his congressional testimony that "if an amendment were unduly to restrict the ability of law enforcement to quickly and efficiently determine the *general location* of a terrorist, kidnapper, child predator, computer hacker, or other dangerous criminal, it would have a very real and very human cost." *Id.* at 6.

92. Mr. Baker's testimony does not cite to specific examples where the DOJ believes courts have conflated cell site information with more GPS location information. *See id.* at 7.

confusion is becoming even more pervasive with regard to historical cell site data. Lower courts are now beginning to split over the proper access standard to apply to it as well. In this context, as with prospective cell site location data, 18 U.S.C. § 2703(c) permits the government to compel "a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the government entity . . . obtains a court order for disclosure under subsection (d) of this section."[93] Stated more simply, a D Order "compels [production of] all non-content records."[94]

1. The DOJ's Interpretation of the Standard for Obtaining Historical Cell Site Data

The DOJ takes the position that historical cell site information satisfies each of the three elements necessary to fall within the scope of 18 U.S.C. § 2703.[95] First, a cell phone company is a provider of "electronic communications service" to the public.[96] Second, "cell site information constitutes 'a record of other information pertaining to a subscriber or to a customer of such service (not including the contents of communications).' "[97] More specifically, historical cell site information "is a record stored by the provider concerning the particular cell tower used by a subscriber to make a particular cell phone call, and is therefore 'a record or

93. 18 U.S.C. § 2703(c) (2010).

94. 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, 1222 (2004).

95. Brief for the United States at 8–9, *In re* the Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't (*Appeal of In re W.D. Pa. Application*), 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866618.

96. *Id.* at 10. The Wiretap Act and SCA define electronic communication service ("ECS") to mean "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. §§ 2510(15), 2711(1). Cell phone service providers provide their customers with the ability to send "wire communications," and thus they are providers of electronic communications service. *See* § 2510(1), (15). Moreover, the DOJ takes the position that:

> [a] "wire communication" necessarily involves the human voice. *See* § 2510(1) (defining "wire communication") and § 2510 (defining "aural transfer"); S. Rep. No. 541, 99th Cong., 2d Sess. 11 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3565 ("cellular communications—whether they are between two cellular telephones or between a cellular telephone and a 'land line' telephone—are included in the definition of 'wire communications' and are covered by the statute").

Brief for the United States, *supra* note 95, at 11 n.10.

97. Brief for the United States, *supra* note 95, at 11.

other information pertaining to a subscriber or customer.' "[98] Finally, "cell site information is non-content information, as it does not provide the content of any phone conversation the user has had over the cell phone."[99] Based on this analysis, prosecutors and agents regularly use D Orders to compel historical location information from third-party providers.

2. Judicial Interpretation of the Standard for Obtaining Historical Cell Site Data

Lower courts have, for the most part, accepted the government's use of a D Order to compel historical cell site information.[100] However, one circuit court has held that there may be circumstances in which a judge can require a probable cause showing before authorizing a government-compelled disclosure of historical cell site information.

a) The Third Circuit Finds That Magistrate Judges Have the Discretion To Require Probable Cause

A government appeal of a magistrate judge's opinion[101] denying the use of a D Order to compel historical cell site data led the Third Circuit to consider whether a D Order based on "specific and articulable facts" can be sufficient to allow the government to compel the production of historical cell site data and whether, in some cases, a court should apply the Fourth Amendment's probable cause requirement in place of the more relaxed provisions of the SCA governing the disclosure of historical cell site information.[102] The Third Circuit held that historical cell site data "is obtainable under a § 2703(d) order and that such an order does not require

98. *Id.* (citing *In re S.D.N.Y. Application*, 405 F. Supp. 2d 435, 444 (S.D.N.Y 2005), and noting that cell site data is "information" and " 'pertain[s]' to a subscriber or customer of cellular telephone service").

99. *Id.* (citing 18 U.S.C. § 2510(8) and defining the "contents" of communications to include information concerning its "substance, purport, or meaning").

100. *See In re* Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 82 (D. Mass. 2007) (granting the government's application for historical cell site information based on the government's statutory analysis of 18 U.S.C. §§ 2703(c), (d)); *id.* at 79 n.5 (collecting cases where courts have assumed or applied in dicta that compelling disclosure of historical cell site data is proper under § 2703(d) of the SCA).

101. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't (*In re W.D. Pa. Application*), 534 F. Supp. 2d 585 (W.D. Pa. 2008). On appeal from the Magistrate Judge to the District Court, the court "recognized 'the important and complex matters presented in this case,' but affirmed in a two page order without analysis." *Appeal of In re W.D. Pa. Application*, 620 F.3d 304 (3d Cir. 2010) (citing *In re W.D. Pa. Application*, 534 F. Supp. 2d 585).

102. *Appeal of In re W.D. Pa. Application*, 620 F.3d 304.

the traditional probable cause determination."[103] The Third Circuit also found, however, that magistrate judges have the discretion to turn down a government application for a D Order even when the D Order standard has been satisfied and, instead, require a probable cause showing. This determination is based upon the Third Circuit's reading of D Order statutory language as "language of permission rather than mandate."[104] The extent to which a magistrate judge has discretion to deny a D Order is unclear, as the opinion merely instructs that the option to require a warrant "be used sparingly because Congress also included the option of a § 2703(d) order," that judges do not have "arbitrary" discretion, and in those cases where a magistrate judge does require a warrant, she must "make fact findings and give a full explanation that balances the government's need (not merely desire) for the information with the privacy interests of cell phone users."[105]

In his concurring opinion, Judge Tashima noted his agreement with most of the reasoning of the majority opinion, but he was concerned that "contradictory signals" leave magistrate judges and prosecutors with a lack of "standards by which to judge whether an application for a § 2703(d) order is or is not legally sufficient."[106] Judge Tashima explained that "the majority suggests that Congress did not intend to circumscribe a magistrate's discretion in determining whether or not to issue a court order, while at the same time, acknowledging that [o]rders of a magistrate judge must be supported by reasons that are consistent with the standard applicable under the statute[.]' "[107] Contrary to the majority's statement that "a magistrate judge does not have arbitrary discretion," Judge Tashima suggests that the majority's opinion perpetuates exactly that, because:

> it provides *no* standards for the approval or disapproval of an application for an order under § 2703(d) . . . [and it] vests magistrate judges with arbitrary and uncabined discretion to grant

103. *Id.* at 313.

104. *Id.* at 316 ("We begin with the text. Section 2703(d) states that a 'court order for disclosure under subsection (b) or (c) *may be* issued by any court that is a court of competent jurisdiction and *shall* issue *only if*' the intermediate standard is met. 18 U.S.C. § 2703(d) (emphasis added). We focus first on the language that an order 'may be issued' if the appropriate standard is met. This is the language of permission, rather than mandate. If Congress wished that courts 'shall,' rather than 'may,' issue § 2703(d) orders whenever the intermediate standard is met, Congress could easily have said so. At the very least, the use of 'may issue' strongly implies court discretion, an implication bolstered by the subsequent use of the phrase 'only if' in the same sentence.").

105. *Id.* at 316, 319.

106. *Id.* at 320 (Tashima, J., concurring).

107. *Id.*

> or deny issuance of § 2703(d) orders at the whim of the magistrate, even when the conditions of the statute are met.[108]

Indeed, the very instability that currently plagues the prospective cell site data legal landscape might also "fester" with respect to historical access standards if the Third Circuit's "rule," giving magistrate judges discretion to deny a D Order without standards or guidance about when such denial is appropriate, were to become the law of the land.[109]

In the wake of the Third Circuit's opinion, some magistrate judges who once granted access to historical cell site data with a D Order are now revisiting that practice. In Magistrate Judge Smith's recent opinion, however, the court placed more significance on "new technology" that has "altered the legal landscape even more profoundly than the new caselaw."[110] Judge Smith's opinion meticulously documents the changes in technology leading to his determination that "court decisions allowing the Government to compel cell site data without a probable cause warrant were based on yesteryear's assumption that cell site data (especially from a single tower) could locate users only imprecisely."[111] After establishing the state of current technology and its rapid pace of change in the direction of increased accuracy for the factual record, Judge Smith conducted a constitutional analysis and ultimately concluded that a compelled *warrantless* disclosure of sixty days of historical cell site data violates the Fourth Amendment.[112]

b) The D.C. Circuit's "Mosaic Theory"

Prior to Judge Smith's opinion, Magistrate Judge Orenstein, another judge who previously granted requests for historical cell site data pursuant to a D Order, also denied the government's application absent a warrant based

---

108. *Id.*

109. For a more extended analysis and critique of the Third Circuit opinion, see Orin S. Kerr, *Third Circuit Rules That Magistrate Judges Have Discretion To Reject Non-warrant Court Order Applications and Require Search Warrants To Obtain Historical Cell Site Records*, VOLOKH CONSPIRACY (Sept. 8, 2010), http://volokh.com/2010/09/08/third-circuit-rules-that-magistrate-judges-have-discretion-to-reject-court-order-application-and-require-search-warrants-to-obtain-historical-cell-site-records/.

110. *In re* Application of the U.S. for Historical Cell Site Data (*In re 2010 S.D. Tex. Application*), 747 F. Supp. 2d 827 (S.D. Tex. 2010).

111. *Id.* at 830.

112. The court's reasoning can be summarized as follows: (1) under current location technology, cell site information reveals non-public information about constitutionally protected spaces; (2) historical cell site records are subject to Fourth Amendment protection under the prolonged surveillance doctrine of *United States v. Maynard*, 615 F.2d 544 (D.C. Cir. 2010); and (3) the government has not demonstrated that the location data sought was voluntarily conveyed by the user and therefore *Smith v. Maryland*, 442 U.S. 735 (1979), does not eliminate a legitimate expectation of privacy.

on a probable cause showing.[113] In finding the government's D Order application for historical cell site data over a fifty-eight-day period to be an unreasonable search and seizure under the Fourth Amendment,[114] Judge Orenstein's opinion relies heavily on a recent D.C. Circuit Fourth Amendment decision, *United States v. Maynard*.[115] The court in *Maynard* considered whether the government's warrantless use of a GPS device placed on a vehicle to track a suspect's movements for twenty-eight days, twenty-four hours a day, was an unreasonable search under the Fourth Amendment. In concluding that the long-term GPS surveillance of movements exposed to public view was a search,[116] the *Maynard* court recognized a novel "mosaic theory" of the Fourth Amendment.[117] Specifically, the court explained:

> Prolonged surveillance reveals types of information not revealed by short term surveillance . . . [and] can reveal more about a person than does any individual trip viewed in isolation . . . . A person who knows all of another's travels can deduce he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[118]

As Professor Orin S. Kerr observes, under the mosaic theory, a court determines whether government conduct is a search "not by whether a particular individual act is a search, but rather whether an entire course of conduct, viewed collectively, amounts to a search."[119] Individual acts that

113. *In re* Application of the U.S. for an Order Authorizing Release of Historical Cell-Site Info. (*In re 2010 E.D.N.Y. Application*), 736 F. Supp. 2d 578 (E.D.N.Y 2010). *But see In re* Application of the U.S. for an Order Authorizing Disclosure of Historical Cell Site Info. for Tel. No. [redacted], Misc. No. 11-449, at 5 (D.D.C. Oct. 3, 2011) (Lamberth, C.J.), *available at* http://legaltimes.typepad.com/files/lamberth_ruling.pdf (holding that a D Order permits the government to compel disclosure of historical location data without a probable cause search warrant and that *Maynard* does not control the question).

114. *In re 2010 E.D.N.Y. Application*, 736 F. Supp. 2d at 582.

115. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *reh'g denied sub nom.* United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010), *aff'd*, 132 S. Ct. 945 (2012).

116. In reaching its decision, the court explained how the reasoning of *Knotts* did not foreclose the conclusion that long-term surveillance constitutes a search. *Maynard*, 615 F.3d at 556–58. Indeed, the Court interpreted the *Knotts* opinion as reserving the question of whether *prolonged* use of a beeper device would require a warrant. *Id.* at 556. The court acknowledged, however, that appellate courts in three other circuits have reached opposite conclusions under *Knotts*. *Id.* at 557–58.

117. *Id.* at 562.

118. *Id.* (footnote omitted).

119. *See* Orin S. Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, VOLOKH CONSPIRACY (Aug. 6, 2010), http://

may not, in their own right, be searches can become searches when committed in particular combinations.[120] Thus in *Maynard*, the court does not look at individual data recordings from the GPS device to determine whether, for example, individual trips are searches.[121] Instead, "the Court examines the entirety of surveillance over a one-month period and views it as one single 'thing' " subject to Fourth Amendment analysis.[122] But at what point would a single act or a series of acts amount to the prolonged surveillance that triggers the mosaic theory and how does a prosecutor, judge, or defense attorney recognize the phenomenon? The *Maynard* court gives no real guidance in this regard.[123] Indeed, the Solicitor General in the government's brief filed in *Jones* (formerly *Maynard*)[124] has argued: "[T]he 'mosaic' theory is unworkable. Law enforcement officers could not predict when their observations of public movements would yield a larger pattern and convert legitimate short-term surveillance into a search. Courts would be hard pressed to pinpoint that moment even in retrospect."[125]

While acknowledging primary factual differences between the real-time GPS vehicle tracking in *Maynard* and the government's application for two months' worth of historical cell site data, Judge Orenstein finds the *Maynard* opinion "persuasive" support for his analysis that the Fourth Amendment

volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/.

120. *Id.*

121. *Id.*

122. *Id.*

123. In *United States v. Cuevas-Perez*, 640 F.3d 272 (7th Cir. 2011), the Seventh Circuit considered whether *Maynard* applied to a 60-hour, "factually straightforward" warrantless GPS surveillance. *Id.* at 274. In determining that *Maynard* did not apply to the case, the majority opinion reasoned that *Maynard*'s 28-day surveillance was much lengthier than the 60-hour surveillance before the Seventh Circuit and the "single trip" in the instant case did not "expose or risk exposing" the "twists and turns" of the defendant's life, "including possible criminal activities, for a long period." *Id.* at 274. In concluding *Maynard* did not apply, however, the majority emphasized "the present case . . . is not meant to approve or disapprove the result the D.C. Circuit reached under the facts of that case." *Id.* at 274 n.3. The concurring and dissenting opinions in *Cuevas-Perez* do provide some analysis of *Maynard*. Indeed, the concurring opinion generally finds *Maynard's* mosaic theory "unworkable," with Judge Flaum indicating that it is not "obvious" to him where the *Maynard* Court would "draw constitutional lines around Cuevas-Perez's sixty-hour journey." *Id.* at 282. In contrast, Judge Wood's dissent rejects the majority's "single trip" description, finding much more similarity between Cuevas-Perez's "60 hour odyssey across 1,650 miles" and the prolonged surveillance in *Maynard*. *Id.* at 293.

124. *See supra* note 115.

125. Brief for the United States at 14, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 3561881. Indeed, Respondent Jones does not employ the *Maynard* "mosaic theory" in his brief to the Supreme Court. *See* Brief for Respondent Antoine Jones at 45, *Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 4479076.

requires the government to obtain a warrant to compel the location information.[126] Lower courts' reliance on *Maynard*'s "mosaic theory," however, raises questions, once again, about the viability of a series of cases that give prosecutors and judges little to no guidance about when and what amount of location data is subject to Fourth Amendment protection. Judge Orenstein, for example, found that fifty-eight days of historical cell site data required a warrant under the reasoning in *Maynard* but, in a later opinion applying *Maynard*, he granted an application for discreet amounts of data spanning a twenty-one-day period under a D Order.[127] While such opinions may be heralded as a "victory" for privacy interests because, among other things, they have the effect of destabilizing the government's use of the D Order, they serve neither privacy nor law enforcement interests insofar as they perpetuate a legal landscape in which lower courts continue to "search," in vain, for the appropriate standards to apply.

3. The Jones *Decision*

Notwithstanding such criticism of the mosaic theory in *Maynard*, the concurring opinions in *United States v. Jones*[128] suggest that, in some future case, there may be five votes for a mosaic-type Fourth Amendment theory holding that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[129] Indeed, Justice Alito's

126. *In re 2010 E.D.N.Y. Application*, 736 F. Supp. 2d 578, 584 (E.D.N.Y. 2010). This Article does not focus on appropriate standards for law enforcement use of GPS tracking devices installed on vehicles—which do not involve compelled disclosures from third-party ECPA-covered providers—and which, therefore, as a matter of policy, may implicate slightly different equities and interests for Congress to consider when drafting legislation.

127. *In re* Application of the U.S. for an Order Authorizing Release of Historical Cell-Site Info., No. 11-MC-0113, 2011 WL 679925 (E.D.N.Y. 2011). The government's application for historical cell site data sought information from one phone for a three-day period, a six-day period from the same phone commencing less than a month later, and a twelve-day period from a second phone believed to have been used in furtherance of the offenses under investigation. *Id.* at *1. The court distinguished the result of the instant case from that of *Maynard* primarily because the court could not "assume that the information gleaned over such shorter periods, separated by breaks of weeks or months, would necessarily be as revealing as the sustained month-long monitoring at issue in *Maynard*." *Id.* at *2. In making this distinction, however, the court acknowledged that "any such line drawing is, at least to some extent, arbitrary and the need for such arbitrariness arguably undermines the persuasiveness of *Maynard*, and of [this court's] prior decisions." *Id.* For further analysis and critique of this decision, see Orin S. Kerr, *Applying the Mosaic Theory of the Fourth Amendment to Disclosure of Stored Records*, VOLOKH CONSPIRACY (Apr. 5, 2011), http://volokh.com/2011/04/05/applying-the-mosaic-theory-of-the-fourth-amendment-to-disclosure-of-stored-records/.

128. 132 S. Ct. 945 (2012).

129. *Id.* at 964 (Alito, J., concurring). Justices Ginsburg, Breyer, and Kagan joined Justice Alito's concurrence. While Justice Sotomayor did not join the Alito concurrence, she states

concurrence invokes the novel aggregative Fourth Amendment theory first articulated by the D.C. Circuit in *Maynard*. The Alito concurrence posits that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable" while law enforcement's "secretly monitor[ing] and catalogu[ing] every single movement of an individual's car for a very long period" does not accord with reasonable expectations of privacy.[130] Likewise, *Maynard* previously recognized that "[p]rolonged surveillance reveals types of information not revealed by short term surveillance."[131]

While Justice Alito's concurrence applies the *Katz*[132] "expectation-of privacy test," the majority opinion, authored by Justice Scalia, bases its holding partially on a trespass theory: "We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.' "[133] Justice Scalia defines the offending conduct further stating "the Government physically occupied private property for the purpose of obtaining information."[134] Consequently, though "[t]respass alone does not qualify [as a search]," a search does occur when it is "conjoined" with "an attempt to find something or to obtain information."[135]

Justice Alito criticizes this approach because, among other things, it "largely disregards what is really important (the *use* of a GPS for long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)."[136] Indeed, the attachment-focused majority opinion does not address instances where the use of GPS solely involves the transmission of radio or other electronic

in her own concurrence, "I agree with Justice ALITO that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' " *Id.* at 955 (Sotomayor, J., concurring). *See also* Orin S. Kerr, *What's the Status of the Mosaic Theory After* Jones*?*, VOLOKH CONSPIRACY (Jan. 23, 2012), http://volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/ (explaining that the mosaic theory "lives").

130. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

131. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *reh'g denied sub nom.* United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010), *aff'd*, 132 S. Ct. 945 (2012).

132. Katz v. United States, 389 U.S. 347 (1967). "As Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing *Katz*, 389 U.S. at 361).

133. *Jones*, 132 S. Ct. 945.

134. *Id.*

135. *Id.* at 951 n.5.

136. *Id.* at 961 (Alito, J., concurring).

signals not enabled by the government's direct physical trespass—such as tracking a target's cell phone.[137] While acknowledging that government tracking though electronic means without actual physical trespass may be "an unconstitutional invasion of privacy," the majority opinion asserts "the present case does not require us to answer that question."[138] Moreover, the majority opinion criticizes the line-drawing problems the Alito concurrence presents:

> [I]t remains unexplained why a 4-week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist?[139]

Indeed, consistent with the difficulties *Maynard* raised, Justice Alito's adoption of a mosaic-type theory provides no significant guidance to law enforcement, judges, and industry about when Fourth Amendment concerns materialize: "We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[140] Rather than creating clarity in the law, the Alito concurrence perpetuates, perhaps even intensifies, the confusion surrounding appropriate law enforcement standards for access to location data.

4. The Importance of Legislative Clarity in the Face of Rapid Technological Change

Scholars and advocates may legitimately disagree about Fourth Amendment theory and about courts' application of the Fourth Amendment to government-compelled disclosures of cell site data. Notwithstanding this constitutional debate, however, the current pace of technological change in this area has given rise to inordinately difficult analytical challenges and highlighted a consequent need for Congress to clarify or amend the law. Chief among these challenges is the current instability in the law created when courts must struggle to find congressional intent in laws that predate the current state of location technology—in short, to find intention in the absence of a stable object. In the face of this ultimately futile search for historical interpretive authority, courts must grapple directly with the legal

137. *Id.* at 953 ("Situations involving merely the transmission of electronic signals without trespass would *remain* subject to the *Katz* analysis.").

138. *Id.*

139. *Id.* (citation omitted).

140. *Id.* at 964 (Alito, J., concurring).

implications that enormously complex and quickly evolving location technologies raise in conjunction with the facts of a given case. Finally, courts must try to perform the foregoing analysis while simultaneously confronting any implications the rapid rate of change in the capabilities of location technology might have upon the reasonable scope of their decisions. To avoid these difficult acts of legal navigation, policymakers should enact laws containing *clear* standards that strike the right balance among law enforcement needs and privacy and industry interests. These standards must also be flexible enough to accommodate the pace of technological change to a degree that renders it a moot consideration in any court's analysis.

C. QUESTIONS RAISED BY THE TWO EXISTING STANDARDS FOR COMPELLING DISCLOSURE OF LOCATION DATA

1. What Does a "D" Order Require the Government To Show?

The call by some advocates for a probable cause standard to govern all law enforcement compelled disclosures of location data is, of course, a recognition that the D Order affords a less stringent showing by law enforcement than that required to meet probable cause.[141] Specifically, to obtain a D Order, law enforcement must provide "specific and articulable facts that there are reasonable grounds to believe" that the information to be compelled "is relevant and material to an ongoing investigation."[142] Some scholars have referred to the D Order standard as a "*Terry*-stop" standard, a reference to *Terry v. Ohio*, where the Supreme Court created the reasonable suspicion standard for sidewalk stop-and-frisk encounters.[143] The *Terry* standard is met "when an officer 'point[s] to specific and articulable facts which, taken together with rational inferences from those facts, evince more

141. *See* H.R. REP. NO. 103-837, at 31 (1994) (indicating that the D Order is "an intermediate standard . . . higher than a subpoena, but not a probable cause warrant").

142. 18 U.S.C. § 2703(d) (2010).

143. 392 U.S. 1, 30 (1968); *see also* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 175–76 (2007) (arguing that the D Order standard, although perhaps intended to be more demanding than the relevance standard required for a subpoena, may not be much different: "[e]ven if *material* is meant to augment *relevant*, it does not add much; materiality, in evidence law, means merely that the evidence be logically related to a proposition in the case"); Freiwald, *supra* note 52, at 692 (discussing that the D Order standard permits much broader inquiries into a much wider range of targets than the probable cause standard); Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 54 MINN. L. REV. 1514, 1521–22 (2010) (noting that the D Order standard "is probably much more stringent than the mere-relevance subpoena standard" and is set by Congress "at a high enough level to prevent police fishing expeditions").

than an inchoate and unparticularized suspicion or hunch of criminal activity.' "[144]

From a practical standpoint, the D Order standard facilitates law enforcement access to non-content records at the early stages of an investigation, when the government is unlikely to meet the higher probable cause standard. In a recent case not involving location information, the DOJ asserted that the D Order standard "derives from the Supreme Court's decision in *Terry*" and thus "is no more onerous than the *Terry* rule."[145] As such, the word "material" in 18 U.S.C. § 2703(d) "does not transform the § 2703(d) standard into one that requires a showing that the records sought are 'vital,' 'highly relevant,' or 'essential.' "[146] Indeed, the scope of a D Order may be "appropriate even if it compels disclosure of some unhelpful information," as " '§ 2703(d) is routinely used to compel disclosure of records, only some of which are later determined to be essential to the government's case.' "[147] For example, if investigators compel location information for every cell phone in the vicinity of a murder scene for a specific period of time, they are likely to obtain *irrelevant* location information about innocent people who just happened to be in a particular place at a particular time in addition to information about the presence of the murderer or witnesses who might have seen the murderer.

Broadening the scope of a request for location information beyond, but in relation to, a known target can advance an investigation strategically. Law enforcement, in certain circumstances, might request the location information of all individuals who were called by or made calls to a particular target.[148] This practice, sometimes referred to as a "community of interest" request, is of particular concern to privacy advocates,[149] but it can, for

144. United States v. Mason, 628 F.3d 123, 128 (4th Cir. 2010) (quoting United States v. Branch, 537 F.3d 328, 336 (4th Cir. 2008)).

145. Government's Response to Objections of Three Twitter Subscribers to Magistrate Judge's March 11, 2011 Opinion Denying Motion To Vacate and Denying in Part Motion To Unseal at 8–9, *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 2011 WL 5508991 (E.D. Va. 2011) (Misc. Nos. 1:11-DM-3, 10-GJ-3793 & 1:11-EC-3), *available at* http://files.cloudprivacy.net/goverment_opp.pdf.

146. *Id.* at 8–9 (quoting Subscribers' Objections).

147. *Id.* at 8 (quoting Magistrate Judge Buchanan's Opinion and Order of March 11, 2011).

148. *See House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 29–30 (written statement of Albert Gidari, Perkins Coie LLP) (explaining that with respect to location information of specific users, many orders now require disclosure of the location of all of the associates who were called by or made calls to a target).

149. Some privacy scholars express strong concerns with a standard that "allows the government to seek location information about apparently innocent parties regularly," noting that community of interest requests provide law enforcement with information about

example, enable law enforcement to identify unknown suspects potentially involved in criminal activity with a known target.[150]

Law enforcement often needs the ability to cast a wider investigative net at early stages of an investigation and, assuming the government's interpretation is correct, the D Order standard facilitates this "over-collection" of information. But insofar as the D Order standard does facilitate an often *necessary* over-collection of information, to what extent does it adequately prevent *unnecessary* over-collection of information? In other words, should not the D Order standard explicitly require that a sufficient nexus exist between the scope of the location information requested and the criminal activity being investigated?

If so, how should this nexus standard be examined by courts? Determining whether an application reflects a time period tailored to the criminal activity being investigated is one inquiry for courts to make in an effort to legitimately cabin the amount of information collected. A single

individuals only tenuously connected to a crime without the judicial oversight that a warrant guarantees. *See* Freiwald, *supra* note 52, at 718.

150. Consider the following scenario: British authorities at an airport package transit x-ray station in Coventry, England x-rayed a package and discovered a .375 Magnum revolver hidden inside a child's toy boat. More packages containing weapons and ammunition concealed inside children's toys were also discovered. When the revolver from the first package was removed, agents noticed that the gun's serial number had been filed down, but forensic analysis reconstructed the number, allowing law enforcement to trace the gun back to a dealer with a known identity and a *female* gun purchaser with a known identity in South Florida. The packages had also been mailed from South Florida via express mail, which allowed agents to identify the location, time, and date that the package was mailed. Cameras inside those post offices recorded video showing two men mailing the first package containing the .357 Magnum revolver. No further information identifying those men was known at the time. It is reasonable to assume that the woman who purchased the revolver (whose identity law enforcement had confirmed) called or was called by the men who mailed the package. One way to assist law enforcement in identifying the men (who continued to mail packages ultimately discovered at Coventry airport) would be to obtain location information focused on the individuals in contact with the known female gun purchaser.

This factual scenario is taken from a real case, *United States v. Claxton*, No. 99-06176 (S.D. Fla. June 13, 2000) (Ferguson, J.), prosecuted by Stephanie in 1999–2000 involving a cell of IRA operatives who came to the United States, purchased weapons illegally, hid them in children's toys and large, hollowed-out computer towers, and mailed them to the Republic of Ireland where they would be smuggled into Belfast. This operation was occurring during a critical time in the peace process and the weapons were intended to replace the cache of weapons being turned over as part of the Good Friday Agreements. The factual narrative described is condensed to illustrate how a "community of interest" request would have assisted in identifying the identities of the men mailing the packages, had such a practice been in use at that time. For more information about the case, see Mike Clary, *Lax Florida Laws Attracted IRA*, REGISTER-GUARD (Eugene, Or.), June 8, 2000, at 6A, *available at* http://goo.gl/S6BgC.

bank robbery occurring over the course of an hour committed by a few suspects, for example, would likely require a narrower collection of information than a sophisticated drug conspiracy covering multiple jurisdictions with multiple conspirators occupying different roles and performing different tasks. Not only would the length of time reflected in the bank robbery D Order application likely be shorter than in the drug conspiracy application, but the number of individuals targeted (known and unknown) might also be fewer. In certain types of investigations, identities of targets are not initially known, but locations where crimes or activities relevant to determining the identities of suspects are known. When the request for the location data is centered on a place where an activity occurred, courts can ensure that the length of the request (i.e., from "Time *X*" to "Time *Y*") is sufficiently tailored to when the investigation suggests that the suspects were present at the location. Similarly, when community of interest requests are made, courts could ensure that the breadth of location information requested about individuals who called or were called by a target is reasonable in light of investigative facts described in the application. There are, of course, many permutations of how the scope of a request for location data would manifest in a particular investigation. Considering that D Orders necessarily facilitate an over-collection of information, however, Congress could amend the language of § 2703(d) to ensure that courts are examining whether a sufficient nexus exists between the scope of the location information requested and the criminal activity being investigated.

2. Probable Cause of What?

A strict probable cause standard for the disclosure of location information could interfere with legitimate law enforcement objectives. Some of the privacy concerns motivating the advocacy for the application of a probable cause standard to all law enforcement compelled disclosures of any and all location information are discussed later in Part V. At this stage in the analysis, however, it is useful to explore how a strict definitional application of the probable cause standard—as articulated in Rule 41[151]—might unduly limit some of the basic law enforcement uses of prospective and historical location information to the degree that legitimate investigative activities

151. *See* FED. R. CRIM. P. 41(c) (listing categories of probable cause: "(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained").

dependent upon the use of these tools would be inhibited, even thwarted, from the start.[152]

If required to obtain a Rule 41 warrant for compelled disclosures of location information, the government would need to establish probable cause to believe that the location information *itself* is evidence of a crime.[153] In some instances, the location of a cell phone, insofar as it reveals a suspect's location, would qualify as evidence of a crime. Location information, for example, may rebut a defendant's alibi, place a defendant at the scene of a crime, or show that a defendant's movements are consistent with activities or overt acts alleged in furtherance of a criminal conspiracy.

But not every use of location information by law enforcement easily fits into the "evidence of a crime" element of Rule 41. If, for example, a person has committed a crime in the past, her current location may not be evidence of a crime, yet there might exist circumstances in which law enforcement has a legitimate need to find her.[154] If law enforcement has evidence to suggest that a person is about to commit a crime, her current location or prospective location leading up to the commission of that crime may or may not, itself, be evidence of a crime, yet our society generally accepts that law enforcement has a legitimate need to prevent her from committing a crime. Indeed, when addressing the DDP proposal that a probable cause warrant should be required for law enforcement access to all location data, Professor Kerr posed the question, "probable cause *of what*?"[155] Is it "probable cause to believe the person tracked is guilty of a crime" or "probable cause to believe the evidence of location information obtained would *itself* be evidence of a crime?"[156] Professor Kerr noted that the difference is important because, in the case of a search warrant, probable cause generally refers to probable

152. We do not claim to know, nor are we able to anticipate, all of the ways in which law enforcement uses prospective and historical location information in investigations.

153. *See In re* Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134, 135 (D.D.C. 2006) (explaining the difference between the D Order standard and probable cause as being that the latter requires a finding that there is probable cause to believe that the information sought is itself evidence of a crime rather than reasonable grounds to believe that the information sought is relevant and material to an ongoing investigation).

154. Some courts, however, have construed the probable cause requirement more broadly with respect to tracking devices or cell site data. *See, e.g.*, *In re* Application of the United States for and [sic] Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 581–82 (W.D. Tex. 2010).

155. *House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 39 (written statement of Prof. Orin S. Kerr, The George Washington Univ. Law Sch.).

156. *Id.*

cause to believe that the information sought is *itself* evidence of a crime.[157] Cell phone location data will be evidence of a crime in only certain kinds of cases and will not normally be evidence of a crime when investigators need to learn the current location of someone who committed a past crime.[158]

Magistrate Judge Susan K. Gauvey amplified this analysis in a recent decision when she concluded that a probable cause search warrant does not permit law enforcement to acquire GPS location information solely to execute an arrest warrant.[159] Specifically, the court noted that the government's "probable cause" theory for obtaining the GPS location data to locate the subject of the arrest warrant was that the "evidence sought will aid in a particular apprehension," not that it was evidence of a crime itself.[160] The government's request was for "broad information concerning [a] defendant's ongoing location" with no alleged relationship whatsoever between the "defendant's ongoing movements and his crime."[161] The court therefore reasoned that, because the government had not established the "requisite nexus between the information sought and the alleged crime, no search warrant may issue" for the location data.[162]

Moreover, in certain circumstances, law enforcement may compel historical location information to *exclude* someone from a criminal investigation. In that instance, the location information would not, under any reasonable stretch of Rule 41, be evidence of a crime but rather would serve the important function of "clearing" someone of criminal activity. Clearing a suspect would thus prevent further investigation, potentially avoiding a needless expenditure of government resources and a gratuitous government intrusion into his life by focusing the investigation more accurately upon the true perpetrator. These are just a few examples of how the "evidence of a crime" element of Rule 41 may not encompass important law enforcement investigative activities. To the extent that good policy may dictate a probable cause standard for location information, that standard would need to accommodate the diverse, legitimate uses of location information by law enforcement.

157. *Id.*

158. *Id.*

159. *In re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., No. 10-2188, 2011 U.S. Dist. LEXIS 85638 (D. Md. Aug. 3, 2011).

160. *Id.* at 93.

161. *Id.* at 105.

162. *Id.*

IV. LESSONS LEARNED

In 2010, the House Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties held three ECPA reform hearings (with Stephanie serving as lead counsel). The second of those hearings, and the most challenging to conceive and execute, explored issues pertaining to law enforcement access of location data (Location Hearing).[163] The hearing focused on supplying members of Congress with the knowledge necessary to clarify or propose new law enforcement access standards for location information.[164]

Some of the challenges Stephanie encountered in developing this hearing stemmed from factual and policy questions and quandaries that continue to inform the search for reasonable access standards and other reforms that will strike the right balance among the interests of law enforcement, consumer privacy, and industry. This Part discusses these challenges, which now motivate and shape the recommendations for the policy framework presented later in this Article.

A. ACQUIRING FACTS TO MAKE GOOD POLICY IS DIFFICULT

Location technology and the uncertain legal landscape governing law enforcement access to location information are complex subjects. As with most complicated issues, Congress needs information from all stakeholders—in this case from law enforcement, consumer privacy and civil liberties advocacy groups, and industry representatives—to judge the relative necessity for legislative action and discern the best directions for policy. When compared, however, with other new technologies prompting Subcommittee consideration of ECPA reform, such as cloud computing, the subject of location-based information and services inspires an unusual degree of secrecy on the part of both industry and law enforcement.

At a later Subcommittee ECPA reform hearing focused on cloud computing, five major cloud computing companies testified.[165] Industry testimony included explanations of business models and services offered by the various cloud companies and a discussion about how current ECPA standards are often difficult to apply to cloud services like Google Docs and

163. *See Location Hearing*, *supra* note 19.

164. *See id.*

165. *See generally ECPA Reform and the Revolution in Cloud Based Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010) [hereinafter *Cloud Based Computing Hearing*], *available at* http://judiciary.house.gov/hearings/printers/111th/111-149_58409.PDF. Industry witnesses included representatives from Google, Microsoft, Salesforce, Rackspace, and Amazon.

Google Calendar.[166] Moreover, some of these companies asserted that weak ECPA privacy protections for information stored "in the cloud," versus the full Fourth Amendment protections afforded information stored on personal laptops, limits the expansion of the cloud market, particularly to foreign customers who are concerned that the U.S. government has overly broad access to cloud-stored information.[167]

In contrast to that very public cloud computing discussion, no wireless carriers or other providers of location-based services to consumers testified at the location hearing. While industry witnesses willingly discussed details about cloud-based services, as well as the challenges the law presents for the industry's compliance with law enforcement requests for information stored in the cloud, no similar public discussion occurred vis-à-vis law enforcement requests for location information or the types of location information carriers collect and retain.

Law enforcement is equally reticent to discuss publicly the investigative practices and processes they employ to obtain location information. While they willingly talk about how critical location information is for a variety of enforcement responsibilities,[168] they will confirm only very general information about the acquisition and uses of the location data. Of course, when overly detailed information about sources and methods becomes public, these sources and methods may cease to be useful investigative tools.[169] But, unlike Wiretaps or Pen/Trap surveillance, Congress does not even have a sense of the number and scope of law enforcement requests for

166. *See id.* at 20 (statement of Richard Salgado, Senior Counsel, Law Enforcement & Info. Sec., Google Inc.).

167. *See id.* at 40 (testimony of David Schelhase, Exec. Vice President & Gen. Counsel, Salesforce.com) (explaining that customers considering storing their information in the cloud want assurances that the U.S. government will not access their data without appropriate due process).

168. *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 5 (testimony of James A. Baker); *see also Location Hearing*, *supra* note 19, at 60–61 (written statement of Richard Littlehale, Assistant Special Agent in Charge, Technical Servs. Unit, Tenn. Bureau of Investigation) (describing how cell phone location information frequently permits law enforcement an opportunity to find and rescue a victim or apprehend an offender in a matter of hours).

169. We are not in a position to assess all of the circumstances where location information as an investigative tool could become less useful to law enforcement upon more disclosure about the method and frequency of this tool. We do note, however, that cellphones are increasingly becoming a necessary tool for society, and as a result, it is extremely difficult to avoid the possibility of location surveillance without turning off a phone, and losing all the benefits of that technology.

location information, statistics that would not necessarily require the exposure of detailed sources and methods.[170]

While we can debate the motivations for the lack of detailed information in the public record about industry and law enforcement practices pertaining to location information, at the end of the day, Congress needs comprehensive information to legislate good policy. For both Wiretap and Pen/Trap authorities, for example, Congress mandated annual Wiretap and Pen/Trap reports, recognizing the need for accurate reporting on law enforcement's use of these tools.[171] As Senator Patrick Leahy has stated, reporting requirements are a "far more reliable basis than anecdotal evidence on which to assess law enforcement needs and make sensible policy in this area,"[172] as well as providing some degree of transparency and oversight of these surveillance powers.[173] No reporting requirements currently exist for location information.[174] Back in 2000, however, the Republican-controlled House Judiciary Committee proposed legislation concerning law enforcement access standards for prospective location information.[175] This bill included new reporting requirements that would have given Congress some sense of the scale of law enforcement compelled disclosures, as well as the number of people whose data was provided to law enforcement.[176] The

170. *See generally* Christopher Soghoian, The Law Enforcement Surveillance Reporting Gap (Apr. 10, 2011) (unpublished manuscript), *available at* http://ssrn.com/abstract=1806628.

171. *See* 18 U.S.C. § 2519(2)–(3) (2010) (outlining what the intercepted communications report issued by the Administrative Office of the United States Courts must contain). These reports are detailed, revealing for each wiretap the city or county where it was executed, the type of interception (phone, computer, pager, fax), the number of individuals whose communications were intercepted, the number of intercepted messages, the number of arrests and convictions that resulted from interception, as well as the financial cost of the wiretap. *See also id.* § 3126.

172. 145 CONG. REC. 30,868 (1999) (statement of Sen. Leahy).

173. S. REP. NO. 90-1097, at 79 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2196 ("[The wiretap reports] are intended to form the basis for a public evaluation of its operation. The reports are not intended to include confidential material. They should be statistical in character. . . . [They] will assure the community that the system of court order electronic surveillance envisioned by the proposed chapter is properly administered and will provide a basis for evaluating its operation.").

174. *See* Soghoian, *supra* note 170, at 22.

175. *See Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 106th Cong. (2000) [hereinafter *House Judiciary 2000 ECPA Hearing*].

176. *See* Digital Privacy Act, H.R. 4987, 106th Cong. (2000). While the DOJ opposed the particular formulation of these reporting requirements because they were overly burdensome, they could be structured to be less onerous on investigators and prosecutors. *See House Judiciary 2000 ECPA Hearing*, *supra* note 175, at 51 (statement of Kevin DiGregory, Deputy Assoc. Attorney Gen., Dep't of Justice) ("[T]he imposition of such extensive

bill did not become law and now, more than ten years later, Congress has little more information than it did in 2000.[177]

B. THE SINGULAR ADVOCACY FOCUS ON LAW ENFORCEMENT STANDARDS HAS NARROWED A DISCUSSION THAT SHOULD INCLUDE MINIMIZATION AND OTHER "DOWNSTREAM" PRIVACY PROTECTIONS

The advocacy regarding the appropriate standard for law enforcement access to location information has largely focused on the DDP Coalition principle calling for a Rule 41 probable cause requirement for all law enforcement compelled disclosures of location information (historical and prospective, regardless of accuracy).[178] This unitary standard, however, is a "non-starter" for law enforcement insofar as it will unduly limit the acquisition of non-content information at the early stages of an investigation and will likely prohibit some basic investigative uses of location information.[179] Indeed, it is one side of what has appeared to become a rather intractable stalemate.

The singular advocacy focus on a "high" law enforcement access standard unduly limited a discussion of other downstream, post collection privacy protections, which were neither included in the DDP proposal nor adequately considered publicly. Such additional protections are a significant component, along with reasonable access standards, in the broader privacy framework proposed in Part VI. Such measures, mandated by Congress for other surveillance authorities, include: minimization, a process by which information not relevant to the investigation is purged from law enforcement databases;[180] notice to individuals whose location information has been disclosed to law enforcement at a time that does not harm an ongoing investigation;[181] and the publication of statistical reports on law enforcement use of location surveillance authorities.[182] These sorts of protections are one

reporting requirements for cyber-crime investigators would come at a time when law enforcement authorities are strapped for resources to fight cyber-crime. The reporting requirements for wiretaps, while extensive, are less onerous because law enforcement applies for such orders relatively rarely. Extending such requirements to orders used to obtain mere transactional data would dramatically hinder efforts to fight cyber-crime, such as the distribution of child pornography and Internet fraud.").

177. *See* Soghoian, *supra* note 170, at 23.

178. *See Our Principles*, *supra* note 22.

179. *See supra* Part III.

180. *See* 18 U.S.C. § 2518(5) (2010); 50 U.S.C. § 1804(a)(5) (2009); *id.* § 1861(b)(2)(B).

181. *See* 18 U.S.C. § 2518(8)(d) (1998).

182. *See* 18 U.S.C. § 2519 (2010).

way to balance or offset access standards authorizing broader law enforcement collection of data.

C. THE POLARIZED VIEWS OF LAW ENFORCEMENT AND PRIVACY ADVOCATES MAKE CONSENSUS BUILDING DIFFICULT

It is not particularly insightful to observe that when one side of a debate starts from a position that is completely unworkable for the other side and will not move, it is difficult to build consensus. If, at the end of the day, the only standard for location data that is acceptable to privacy advocates is a Rule 41 probable cause standard, then they risk letting the proverbial perfect be the enemy of the good. The advocacy message for overall ECPA reform—while supported through industry participation in the DDP Coalition and echoed by strong industry voices outside of the coalition calling for Congress to enact clear legal rules and shelter industry from liability—was driven primarily by privacy advocates. Thus, the burden to suggest new, workable, and more privacy-protective standards falls primarily on the shoulders of the community of privacy advocates. This is not an area where law enforcement will likely act as a willing catalyst for new access standards that place restrictions on their own investigative tools in the name of better privacy protections, even if they are prepared to agree to a fair compromise in the end. Moreover, law enforcement has strong advocates in Congress who will fight against overly broad proposals to restrict investigative authorities. Consider, for example, the opening statement by then Ranking Member Sensenbrenner (now Chairman of the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security and author of the USA PATRIOT Act) at the Location Hearing. Having clearly read the proposal for a unitary probable cause standard, the Ranking Member announced, "While there may very well be a need to clear up the confusion in the area of obtaining prospective cell site information, it does not necessarily follow that the appropriate remedy to any ambiguity would be a Rule 41 search warrant based upon probable cause."[183]

Notwithstanding such strong allies in Congress, however, the DOJ should carefully measure the practical impact of *Jones*. While *Jones* does not hold that a warrant is required for the installation and use of a GPS tracking device,[184] a prudent prosecutor interested in ensuring that GPS tracking

183. *Location Hearing*, *supra* note 19, at 3 (opening statement of ranking member Rep. Jim Sensenbrenner).

184. The Court declined to reach the question of whether a warrant is required to install a GPS device. *See* United States v. Jones, 132 S. Ct. 945, 954 (2012) ("The Government argues in the alternative that even if the attachment and use of the device was a search, it was reasonable—and thus lawful—under the Fourth Amendment because 'officers had

evidence is admissible at trial would, absent further judicial or congressional guidance, be wise to obtain one in every instance. Only time will tell whether this new strategic necessity will have a measurable adverse impact on law enforcement investigations.

A more urgent concern for the DOJ, however, should be the threat of continued judicial application and expansion of the mosaic theory inspired by the signals in the *Jones* concurrences. The signals in the *Jones* concurrences indicate that a majority of the Court could, in the future, incorporate some version of the theory into its Fourth Amendment jurisprudence. As we have seen, absent clear congressional guidance regarding standards for law enforcement access to location data, some courts are already applying the mosaic theory to government applications for historical cell location data with varying interpretations about how much data forms a mosaic and triggers a Fourth Amendment issue.[185] Justice Alito's answer for how to deal with the thorny line drawing problem under a theory that does not define when the mosaic materializes is simple: "where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment Search, police may always seek a warrant."[186] But this simple dictate is hardly a viable one for law enforcement in every instance.[187] If the DOJ finds this potential reality to be unworkable and harmful to future law enforcement investigations (as it has suggested in congressional testimony),[188] it should engage earnestly in the legislative process and be prepared to agree to some reasonable additional privacy protections. Indeed, the prospect of a majority that would make the mosaic

reasonable suspicion, and indeed probable cause, to believe that [Jones] was a leader in a large-scale cocaine distribution conspiracy.' We have no occasion to consider this argument. The Government did not raise it below, and the D.C. Circuit therefore did not address it." (citation omitted)); *see also* Orin S. Kerr, *What* Jones *Does* Not *Hold*, VOLOKH CONSPIRACY (Jan. 23, 2012), *available at* http://volokh.com/2012/01/23/what-jones-does-not-hold/ ("[W]e actually don't yet know if a warrant is required to install a GPS device; we just know that the installation of the device is a Fourth Amendment 'search.' ").

185. *See supra* Section III.B.2.b.

186. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

187. *See supra* Section III.A.3.

188. *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 5 (testimony of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice) ("If an amendment [to ECPA] were to unduly restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker or other dangerous criminal, it would have a very real and very human cost.").

theory the law of the land should concentrate the Department's mind wonderfully upon resolving this issue through the legislative process.[189]

V. WHAT IS THE HARM, AND WHO CAN ADDRESS IT MOST EFFECTIVELY?

In proposing that Congress reform existing location privacy law, we confront a logical threshold question: just what harms would we seek to prevent? When it first enacted the Electronic Communications Privacy Act back in 1986, Congress sought to reestablish the balance of interests between law enforcement and privacy[190] that had been upset—to the detriment of privacy—by advances in wireless and computing technologies.[191] Congress also recognized that consumers might not embrace new technologies if privacy interests were not appropriately protected.[192] As technology continues to develop—simultaneously enriching our lives and facilitating more prevalent government (and private) surveillance—Congress, once again, is preparing to confront the task of establishing an appropriate balance among stakeholder equities,[193] which prompts us, yet again, to ask this threshold question.

In recent years, prominent judges have, in written opinions, described and voiced concern over the harms associated with modern location tracking technologies. In doing so, they have suggested that Congress, not the judiciary, might be in the best position to provide appropriate incentives and

189. "Depend upon it, Sir, when a man knows he is to be hanged in a fortnight, it concentrates his mind wonderfully." JAMES BOSWELL, LIFE OF JOHNSON 849 (Oxford Univ. Press 1960) (1791).

190. *See House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 8–9 (written statement of James X. Dempsey, Vice President for Pub. Policy, Ctr. for Democracy & Tech.) (discussing balance of interests Congress sought to strike in enacting ECPA).

191. Among the developments noted by Congress were "large-scale electronic mail operations, cellular and cordless phones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of digitized networks . . . ." H.R. REP. NO. 99-647, at 18 (1986). Privacy, Congress concluded, was in danger of being gradually diminished as technology advanced. S. REP. NO. 99-541, at 2–3, 5 (1986); *see also* H.R. REP. NO. 99-647, at 18 (stating that "legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology").

192. *See* S. REP. NO. 99-541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems"); *see also* H.R. REP. NO. 99-647, at 19 (noting that legal uncertainty over confidentiality "may unnecessarily discourage potential customers from using . . . [new] systems").

193. As of the writing of this Article, five separate hearings on ECPA reform were held during the 111th and 112th sessions of Congress (three hearings held in the House Judiciary Committee and two hearings in the Senate Judiciary Committee).

remedies. We take our cue from these judges and their stated concerns to identify potential harms Congress should consider when it evaluates the relative necessity for legislative action and discerns the best policy direction.[194]

A. THE GOVERNMENT'S GAZE AND THE PANOPTIC EFFECT

As we shall see, some judges who have considered cases involving law enforcement access to location data posit that the persistent gaze of government may itself represent an objective harm to the public.[195] In doing so, these judges have alluded to surveillance theories found in literature, social theory, and philosophy. To evaluate and discuss their conclusions fully, we must briefly describe some of that material and how it appears, directly or allusively, in their opinions.

Late eighteenth-century theories of surveillance as an instrument to administer discipline and enforce social control, such as Jeremy Bentham's "Panopticon" prison architecture,[196] suggest that the potency of the government's gaze is such that, when imposed strategically and with suggested if not actual universality and constancy, it becomes internalized in the very minds of those subjected to its influence as a mechanism of rehabilitative discipline.[197] Moreover, Bentham envisioned the Panopticon's design as appropriate not only to prisons, but to any environment where enhanced discipline is desired: schools, asylums, factories, and more. In short, for Bentham, the panoptic gaze of the state could serve as a secular version of the all-seeing eye of the Judeo-Christian God, and the normative behavioral conformity religious conscience once inspired would be supplanted on more certain ground by the discipline this modern gaze could inspire.

The twentieth-century French social theorist Michel Foucault rigorously analyzed Bentham's project in the Panopticon and expanded it into an interpretive metaphor for coercive social power. Foucault examines "Panopticism" as an instance of modern society's ability to compel

194. What follows in this Section is not an attempt to describe an authoritative legal or philosophical theory of the harms inherent in unjustified disclosure of location data, though we shall have occasion to allude to law, philosophy, and literature in service of the task of describing those harms as expressed by judges who have confronted them and chosen to discuss them in recent opinions.

195. *See* United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring) ("The constitutional ill of prolonged or mass use of GPS technology would not necessarily be based on the information acquired by the device but on the fact of the government's gaze.").

196. *See* JEREMY BENTHAM, THE PANOPTICON WRITINGS 29–95 (Miran Bozovic ed., 1995) (1787).

197. *Id.*

compliance with its approved behavioral norms through its institutions and their various discourses.[198] The presence of modern surveillance mechanisms, visible and imperceptible, public and private, promotes the "Panoptic effect"—a general sense of being omnisciently observed. The state may choose to deploy this effect to amplify and mystify the power of its own "gaze" as a coercive instrument, and to promote the internalization of that gaze in the service of discipline.[199]

Bentham's plan for the Panopticon was fairly simple: a model prison consisting of a central tower surrounded by a ring of prison cells, each of them backlit, so that anyone in the tower could see all of the prisoners at once. Bentham posited that a single inspector in the tower could control the behavior of all of the prisoners through making each prisoner "always feel themselves as if under inspection, at least as standing a great chance of being so."[200] Eventually, since the backlit cells and the tower structure made it impossible for prisoners to observe him, the monitor in the tower would actually become superfluous and the inmates, having internalized the presumption of his continued surveillance, would literally *watch themselves*.

198. *See* MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 195–228 (1978). Discourse in this case does not refer merely to the word's common denotation as written or spoken communication or debate, but to the word as used in modern social theory, particularly the work of Foucault, referring to the various systems of linguistic usages associated with complex social practices (e.g., law, medicine, religion) deployed as instruments of social power, particularly the power of the state. *See generally* MICHEL FOUCAULT, THE ORDER OF THINGS (1970); MICHEL FOUCAULT, THE ARCHEOLOGY OF KNOWLEDGE (1972). For an extended discussion of the diffuse nature of power in society and the role this concept of discourse plays in analyzing how ideas and language encode power in social spaces and, therefore, have the potential to play a role in historical change, see MICHEL FOUCAULT, *Two Lectures*, *in* POWER/KNOWLEDGE: SELECTED INTERVIEWS & OTHER WRITINGS 78 (Colin Gordon ed., 1980).

199. It is important to note that more recent writers on "surveillance theory" have qualified Bentham and Foucault usefully. *See, e.g.*, GILLES DELEUZE, POSTSCRIPT ON THE SOCIETIES OF CONTROL 3–7 (1992) (distinguishing Foucault's "disciplinary" society from his own "control" society in critique of the Panopticon); DAVID LYON, THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND (2006); DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 54–62 (2007) (summarizing contemporary criticism qualifying the application of Foucault's analysis to contemporary surveillance). While the rigor and depth of recent surveillance theory is indispensible background to anyone who would consider surveillance in all its profundity, its presence in legal opinions to date, which is the focus in this Article, has been predominantly restricted to metaphorical allusions to Orwell's dystopia in *1984* and some consideration of the government's "gaze" as discussed in Foucault's interpretation of the Panopticon. Since these interpretive frames are effectively canonical and, as such, disseminated commonly enough to drive judicial decision making, as well as the appeal by the judiciary for legislation in this area, we place our own main focus on them at this moment in the policy debate.

200. Jeremy Bentham, *Letter V: Essential Points of the Plan*, *in* BENTHAM, *supra* note 196.

Foucault claimed this internalization of surveillance made the Panopticon a quintessential figure for a peculiarly modern and secular form of state power that arose in the Enlightenment, "a new mode of obtaining power of mind over mind, in a quantity hitherto without example."[201]

As modern location surveillance techniques increase in precision and their pervasive distribution throughout society becomes known, though the instruments themselves may or may not remain invisible, people become increasingly aware of, and potentially influenced by, a palpable sense of the omniscient gaze similar to that produced by Bentham's prison design.

Consider, for example, that through the use of modern surveillance technologies, a single police officer can now monitor the movement of tens, even hundreds, of targets from the comfort of her desk[202] and, because there is no statutory notice provided to those under such surveillance, targets have no way of knowing if and when they are being or have been watched.[203] While surveillance has traditionally been very expensive in terms of human resources (often requiring multiple shifts of agents to watch a single target for a twenty-four-hour period), the ubiquity of cellular phones and innovations in GPS tracking technology has made surveillance easier, cheaper, and consequently more prevalent.[204] A law enforcement agency's gaze is no longer limited by the number of agents available to drive around a city, but only by the amount of money available in its budget to pay wireless carriers for their assistance, or to purchase GPS tracking devices or other similar technologies.[205] Moreover, although such surveillance is supposed to

201. *Id.* at Preface.

202. United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing en banc).

203. *See Appeal of In re W.D. Pa. Application*, 620 F.3d 304, 317 (3d Cir. 2010) (noting that "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information").

204. *See* United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) ("The new [surveillance] technologies enable, as the old (because of expense) do not, wholesale surveillance. . . . Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive.").

205. Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J.L. SCI. & TECH. 191, 222–23 (2011). ("Many telecommunications companies and ISPs seek and typically receive payment from government agencies for the surveillance services they provide, a practice that the law often permits."). The cost of location surveillance by some carriers appears to have plummeted over the past decade—a savings that they were obligated to pass on to law enforcement, though no public data exists for comparison. For example, in 2003, Nextel communications charged $150 per "ping." *See* NEXTEL, SUBPOENA & COURT ORDERS: NEXTEL'S GUIDE FOR LAW ENFORCEMENT 6 (2003), *available at* http://info.publicintelligence.net/nextelsubpoena.pdf. In 2009, it was revealed that law enforcement agencies had performed 8 million pings

be invisible, it is becoming more perceptible through media stories, making the fact of its pervasive existence known, at least in an abstract sense.[206] This simultaneous visible and invisible presence of surveillance is precisely what produces the anxiety that is the foundation of the panoptic effect.[207] These particular location technologies partake of a whole system of surveillance instruments and mechanisms, both governmental and private, which construct and project the government's gaze.[208]

Echoing the conclusions hinted at by the history of surveillance, its coercive utility, and the rapid innovation in contemporary surveillance technology, including geolocation systems, Seventh Circuit Judge Flaum, while criticizing the reasoning of *Maynard* in *Cuevas-Perez*, suggests that the fact of the "government's gaze" itself, as exerted by "mass use of GPS

via a website created by Sprint/Nextel. *See Pineda-Moreno*, 617 F.3d at 1125 (Kozinski, J., dissenting from denial of rehearing en banc). Although we have no direct evidence to suggest that the carrier has reduced the cost of its pings (or moved to a fixed fee, rather than per-ping charges), even without adjusting for inflation, had Sprint charged $150 for each of the 8 million pings, it would have made $1.2 billion. Since law enforcement certainly did not spend that much money for this purpose, some new billing arrangement must have motivated the increased activity level.

206. *See generally The Wire* (HBO cable television series, 2002–2008); *see also* Anders Albrechtslund, *Surveillance and Ethics in Film:* Rear Window *and* The Conversation, 15 J. CRIM. JUST. & POPULAR CULTURE, no. 2, 2008, at 129–44.

207. Regarding the "Panoptic effect" of the state's gaze, Professor Daniel Solove points out that:

> Although concealed spying is certainly deceptive . . . [i]t is the awareness that one is being watched that affects one's freedom. . . . A more compelling reason why covert surveillance is problematic is that it can still have a chilling effect on behavior. In fact, there can be a more widespread chilling effect when people are generally aware of the possibility of surveillance but are never sure if they are being watched at any particular moment.

DANIEL SOLOVE, UNDERSTANDING PRIVACY 109 (2008). This is true, unequivocally, regarding the specular value of strategically displaying and withholding evidence of state power. Moreover, revelations of the covert commercial use of location-based tools, such as the recently divulged use of Apple's iPhone and Google's Android phones in WiFi mapping, have the indirect effect of reinforcing the general sense of the state's coercive gaze and its power to influence compliance with social norms, whether or not there is any actual convergence of interest between the state and private actors in a given case. *See* Angwin & Valentino-Devries, *supra* note 41.

208. *See* Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, FUTURE CONST. (Brookings Inst., Washington, D.C.), Dec. 8, 2010, *available at* http://www.brookings.edu/~/media/Files/rc/papers/2010/1208_4th_amendment_slobogin/1208_4th_amendment_slobogin.pdf (describing the negative, real world impacts of surveillance even when the government makes no use of the surveillance product).

technology," may represent a "constitutional ill" which amounts to a cognizable harm.[209]

Historical location information produced by mobile devices adds another layer of implication to the panoptic effect. Such information is, of course, a record of where we have been. These data are stored by companies providing wireless services to consumers and on mobile devices for periods of time unknown to the user since retention policies vary by company.[210] Some companies may store more precise data than others,[211] but through these data the government may get an accurate picture of most everywhere we have been.[212] Moreover, once information is disclosed, the government entities responsible for the investigation add it to databases and keep it for an indefinite period of time.[213] In effect, modern location technology can give the government an increasingly perfect memory of our activities, thus making it impossible to escape one's past. Data retention policy, at this point, might be considered a relatively unknown and thus "immature" source of panoptic power. We are only now beginning to learn the details and scope of the heretofore hidden commercial use of location data on smartphones,[214] and Congress is currently considering data retention legislation that will require providers to store subscriber data for twelve months.[215] These developments

209. United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring).

210. Soghoian, *supra* note 205, at 210 ("[M]ost technology providers and communications carriers now have established data retention policies that govern the length of time before which they will delete customer records, communications, logs, and other data. Unfortunately, outside of the search engine market, where pressure from European regulators has led to companies publicly touting their policies, few other firms will publicly reveal their own data retention rules.").

211. *See Location Hearing*, *supra* note 19, at 27 (written statement of Prof. Matt Blaze, Univ. of Pa.).

212. *See* People v. Weaver, 12 N.Y.3d 433, 441–42 (2009) (describing the types of information that tracking devices can record about an individual's life).

213. *See generally* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008). Moreover, the data of innocent individuals who are not targets of government surveillance can get "swept up" by community of interest requests or other compelled disclosures of data that seek to discover everyone who was at or near a particular location at a particular time.

214. *See* Jennifer Valentino-DeVries & Julia Angwin, *Latest Treasure Is Location Data*, WALL ST. J. (May 10, 2011), http://on.wsj.com/xJGP9u ("Location information is emerging as one of the hottest commodities in the tracking industry . . . . [T]he Journal's 'What They Know' series found that 47 of the 101 most popular smartphone apps sent location information to other companies.").

215. The Protecting Children from Internet Pornographers Act of 2011 was favorably reported out of the House Judiciary Committee on July 28, 2011 and requires certain types of providers to retain some types of data for at least 12 months. *See* H.R. 1981, 112th Cong. § 4 (2011), *available at* http://1.usa.gov/xeBBB6.

will inevitably lead to a broader public discussion of both the commercial and law enforcement uses of historical location data. These discussions will ostensibly be conducted in the name of protecting the public from the government's intrusive eye, which will serve ironically to enhance its power to reinforce the panoptic effect.

More than forty years ago, Vice President Hubert Humphrey observed that "[w]e act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change.[216] Justice Douglas made the same point a few years later, observing that "[m]onitoring, if prevalent, certainly kills free discourse . . . ."[217] Humphrey and Douglas both anticipate Foucault in their conclusions in describing the effect of being observed. To these men, one of politics, the other of law, the observing gaze of the state was, intuitively, a powerfully coercive force that changes people, as surely and utterly as the Medusa's gaze was said to change men to stone.

The ever-improving accuracy of location technology has given the government's gaze a degree of clarity hitherto undreamed of, except perhaps in dystopian novels such as Orwell's *1984*. Notably, as they confront the powerful gaze of modern surveillance technologies, judges around the country are voicing their own anxiety regarding the impact of this technology on individuals and society, often turning to sources like Orwell to illustrate their conclusions. In *People v. Weaver*, a case about a GPS tracking device placed on a car, Judge Lippman expressed his concern over the very personal profile of an individual's life captured by tracking technologies:

> The whole of a person's progress through the world, into both public and private spatial spheres, can be charted and recorded over lengthy periods possibly limited only by the need to change the transmitting unit's batteries. Disclosed in the data retrieved from the transmitting unit, nearly instantaneously with the press of a button on the highly portable receiving unit, will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our

216. Hubert H. Humphrey, *Foreword*, *in* EDWARD V. LONG, THE INTRUDERS, at viii (1967).
217. United States v. White, 401 U.S. 745, 762 (1971).

> professional and avocational pursuits. When multiple GPS devices are utilized, even more precisely resolved inferences about our activities are possible. And, with GPS becoming an increasingly routine feature in cars and cell phones, it will be possible to tell from the technology with ever increasing precision who we are and are not with, when we are and are not with them, and what we do and do not carry on our persons—to mention just a few of the highly feasible empirical configurations.[218]

Likewise, in his dissent in *United States v. Pineda-Moreno*,[219] a case where the Ninth Circuit rejected en banc review of a panel decision involving GPS technology, the ever-witty[220] Judge Kozinski turns deadly serious, invoking his own childhood in Communist Romania and alluding directly to the setting of *1984* as he describes the tracking technology in question:

> I don't think that most people in the United States would agree with the panel that someone who leaves his car parked in his driveway outside the door of his home invites people to crawl under it and attach a device that will track the vehicle's every movement and transmit that information to total strangers. There is something creepy and un-American about such clandestine and underhanded behavior. To those of us who have lived under a totalitarian regime, there is an eerie feeling of déjà vu. This case, if any, deserves the comprehensive, mature and diverse consideration that an en banc panel can provide. We are taking a giant leap into the unknown, and the consequences for ourselves and our children may be dire and irreversible. Some day, soon, we may wake up and find we're living in Oceania.[221]

---

218. People v. Weaver, 12 N.Y.3d 433, 441–42 (May 12, 2009).

219. United States v. Pineda-Moreno, 617 F.3d 1120, 1121–26 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing en banc).

220. In criticizing the underlying panel's conclusion that the defendant has no expectation of privacy in his driveway, Judge Kozinski explains:

> The panel authorizes police to do not only what invited strangers could, but also uninvited children—in this case crawl under the car to retrieve a ball and tinker with the undercarriage. But there's no limit to what neighborhood kids will do, given half a chance: They'll jump the fence, crawl under the porch, pick fruit from the trees, set fire to the cat and micturate on the azaleas. To say the police may do on your property what urchins might do spells the end of Fourth Amendment protections for most people's curtilage.

Id. at 1123.

221. *Id.* at 1126. Further, the court in *United States v. Sparks* refused to find a Fourth Amendment violation in the government's use of GPS placed on the defendant's vehicle under the specific facts of the case, but it nonetheless acknowledged that the court "is not unsympathetic to the sentiment expressed by Chief Justice Kozinski and his Ninth Circuit

Judge Kozinski's language echoes the disturbing uncertainty that results when the instruments of the state's panoptic gaze become even partially visible. Indeed, as we have discussed, the very partial nature of their visibility is essential to produce the uncertainty and anxiety of the panoptic effect. In response, Judge Kozinski appeals to a locus of greater authority, here an en banc panel of the Ninth Circuit, to assert the control (i.e., "comprehensive, mature and diverse consideration") necessary to govern the state's panoptic gaze in the name of preserving the specifically "American" way of life it seems to threaten.

Judge Flaum, in his concurring opinion in *Cuevas-Perez*, goes further still, suggesting the government's increasingly powerful and clear sense of sight with regard to the lives of individuals, using new, more accurate location technologies, might offend the Fourth Amendment in a manner explicitly proscribed by the Founders as it was being crafted:

> There may be a colorable argument . . . that the use of GPS technology to engage in long-term tracking is analogous to general warrants that the Fourth Amendment was designed to curtail, because of the technology's potential to be used arbitrarily or because it may alter the relationship between citizen and government in a way that is inimical to democratic society.[222]

brethren, that there is something 'creepy' about continuous surveillance by the government." 750 F. Supp. 2d 384, 395–96 (D. Mass. 2010). While noting that "[a]dvances in technology, like GPS devices, provide neutral and credible evidence and thus facilitate the ultimate (and yet amorphous) goal of 'justice,' " the court also recognizes that "it is easy to envision the worst-case Orwellian society, where all citizens are monitored by the Big Brother government." *Id.* at 394–95; *see also In re* Application of the U.S. Authorizing the Release of Historic Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) ("While the government's monitoring of our thoughts may be the archetypical Orwellian intrusion, the government's surveillance of our movements over a considerable time period through new technologies, such as the collection of cell-site-location records, without the protection of the Fourth Amendment, puts our county far closer to Oceania than our Constitution permits.").

222. United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring). In the same case, in her dissent, Judge Wood also appeals to Orwell for interpretive authority, with a sense of urgency matching that of Judges Flaum and Kozinski:

> This case presents a critically important question about the government's ability constantly to monitor a person's movements, on and off the public streets, for an open-ended period of time. The technological devices available for such monitoring have rapidly attained a degree of accuracy that would have been unimaginable to an earlier generation. They make the system that George Orwell depicted in his famous novel, *1984*, seem clumsy and easily avoidable by comparison.

Id. at 286 (Wood, J., dissenting).

Judge Flaum's concurrence strongly criticizes the reasoning of the *Maynard* court[223] (the case concluding that *United States v. Knotts*[224] does not govern prolonged GPS surveillance and instead applying a mosaic theory of the Fourth Amendment), yet he seems to go out of his way to propose an alternative theory of the Fourth Amendment that might, perhaps, offer a way to cabin or control the government's prolonged use of GPS tracking. This palpable concern on the part of senior jurists from two appellate courts is indicative of the general harm to society, to which all others are ancillary, created by location technology, and the issues this technology raises should be scrutinized accordingly.

But where should one turn for sufficient authority? A Ninth Circuit en banc panel? How about the ultimate authority in the judicial branch: the Supreme Court of the United States? Judge Flaum considers that option briefly, perhaps aware of the government's petition for certiorari in *Maynard*, later granted in *Jones*,[225] in further reducing his argument to its bare bones: "on this view, the constitutional ill of prolonged or mass use of GPS technology would not necessarily be based on the information acquired by the device but on the fact of the government's gaze."[226]

It may be tempting, as a judge on a federal appellate court, to urge the Supreme Court to employ the Fourth Amendment against the "ill" that can be inflicted by the mere "fact of the government's gaze." But Judge Flaum himself, having indulged in the Fourth Amendment argument and perhaps gauging the limited power of the judiciary to use the common law in an effort to assert control of technology changing at the pace of Moore's Law,[227] immediately withdraws it in favor of a legislative remedy:

---

223. *Id.* at 280 (Flaum, J., concurring) ("Neither of *Maynard*'s twin bases for ruling that the defendant had an objectively reasonable expectation of privacy is doctrinally sound—or all that workable as a practical matter.").

224. 460 U.S. 276 (1983) (holding that a person does not have a reasonable expectation of privacy in movements from one place to another on public thoroughfares).

225. *See* Petition for Writ of Certiorari, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259).

226. *Cuevas-Perez*, 640 F.3d at 285 (7th Cir. 2011) (Flaum, J., concurring).

227. Moore's law describes a long-term trend in the development of computer hardware, specifically that the number of transistors that can be placed inexpensively on an integrated circuit doubles approximately every two years, resulting in a corresponding, roughly exponential, increase in the capabilities of many digital devices—processors, computer memory, digital camera resolution, and more. Moore's projected rate of growth, which is used in the semiconductor industry to guide long-term planning and to set targets for research and development, has continued for over fifty years and is expected to remain constant through at least 2015 or later. It was named for Gordon E. Moore, the co-founder of Intel, who described the trend in a 1965 paper. Gorden E. Moore, *Cramming More Components onto Integrated Circuits*, 38 ELECTRONICS, no. 8, Apr. 19, 1965, *available at*

> Of course, the Supreme Court just last term reminded us that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010). In light of *Knott*'s holding and *Quon*'s admonition, it strikes me not so much as insufficiently circumspect as simply beyond our mandate to conclude that what is permissible when accomplished with a beeper is impermissible when accomplished with a GPS unit. I agree with the dissent, however, that nothing would preclude Congress from taking the important questions implicated by GPS technology and imposing answers. Indeed, the unsettled, evolving expectations in this realm, combined with the fast pace of technological change, may make the legislature the branch of government that is best suited, and best situated, to act.[228]

The Supreme Court has now decided *Jones*. Where do we find ourselves? The concurring opinions echo the concerns Judge Kozinski and Judge Flaum expressed. Justice Alito's concurrence recognizes that law enforcement's secret, long-term monitoring of every single movement of an individual's car does not accord with society's reasonable expectations of privacy.[229] Justice Sotomayor even quotes Judge Flaum's concurrence in *Cuevas-Perez* as she asserts: "GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.' "[230]

The majority opinion, however, functions only to limit the scope of the "government's gaze" with respect to the physical attachment and use of a GPS tracking device. Indeed, the majority's definition of "search" does not apply to situations where the transmission of radio or other electronic signals is not attained through the government's physical attachment of a device by trespass. Moreover, Justice Alito's adoption of a mosaic-type theory raises

---

http://download.intel.com/museum/Moores_Law/Articles-Press_releases/Gordon_Moore_1965_Article.pdf. *See generally* Bob Schaller, The Benchmark of Progress in Semiconductor Electronics (Sept. 26, 1996) (unpublished paper), *available at* http://research.microsoft.com/en-us/um/people/gray/Moore_Law.html.

228. *Cuevas-Perez*, 640 F.3d at 285–86 (Flaum, J., concurring) (citing Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004) (arguing that Congress should be the primary driver of privacy protections when technology "is in flux")).

229. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

230. *Id.* at 956 (Sotomayor, J., concurring) (quoting *Cuevas-Perez*, 640 F.3d at 285) (Flaum, J., concurring)).

the same thorny line drawing issues presented by *Maynard*.[231] Perhaps recognizing the limitations of this approach, Justice Alito acknowledges that "[t]he best we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[232] But like Judge Flaum, Justice Alito recognizes that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[233]

Certain judges and justices who have closely considered the implications of location technology have expressed concern, even anxiety, over the effects on society of the government's use of location technologies. Some of these jurists have further questioned the law's current ability to contain its effects and have found that ability, and hence their own powers, wanting. We share the jurists' skepticism. Cognizant of the power of the government's gaze and in agreement with Justice Alito's[234] and Judge Flaum's conclusion that the legislature is likely the branch of government best suited to fashion the appropriate protections against this gaze, we now present our model privacy framework for location information.

VI. LEGISLATIVE PROPOSAL

In an effort to try and bridge the gap between the currently polarized positions of privacy advocates and law enforcement, we offer a model privacy framework to govern law enforcement compelled disclosures of historical and prospective location information.[235] It is neither the most

231. *See supra* Section III.B.2.b.

232. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring). Furthermore, during the government's oral argument in *Jones*, shortly following Justice Breyer's stated concern over "what . . . a democratic society [would] look like if a large number of people did think that the government was tracking their every movement over long periods of time" and his search for a "reason and principle" that would "reject" this kind of government surveillance "but wouldn't also reject [government tracking] 24 hours a day for 28 days," Justice Scalia exclaimed, "Don't we have any legislatures out there that could stop this stuff?" Transcript of Oral Argument at 24–26, *Jones*, 132 S. Ct. 945 (2012) (No. 10-1259), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf.

233. *Id.* (citing Kerr, *supra* note 228, at 805–06).

234. Justice Ginsburg, Justice Breyer, and Justice Kagan all signed Justice Alito's concurrence regarding this conclusion.

235. We intend the privacy framework and access standards proposed in this Part only to apply to criminal law enforcement authorities. They are not intended to amend or affect intelligence or national security authorities that the government may use to acquire location information. The government's use of such intelligence tools is beyond the scope of this Article. Any actual legislation that seeks only to amend criminal law enforcement authorities would include appropriate statutory language to exempt relevant intelligence authorities.

friendly to law enforcement nor the most protective of privacy, but it is an attempt to find a reasonable balance among the interests of law enforcement, privacy, and industry.

Our proposal relies on several overarching principles that form a foundation for crafting the correct balance: a strong privacy framework that does not unduly limit law enforcement investigative activities or negatively affect industry innovation. These principles are influenced by a variety of sources including, but not limited to, ideas expressed by the DDP Coalition, off-the-record discussions with industry representatives, information revealed in public congressional hearings and elsewhere in the public record, and extensive discussions with private practitioners, academics, and privacy advocates.

A. OVERARCHING PRINCIPLES

1. Clear Rules

Law enforcement, judges, and industry all benefit from clear access standards.[236] When the ECPA was passed in 1986, location data was not a "routine tool" used by law enforcement and cell phones were a luxury affordable to only a small number of people. Congress, understandably, did not have the clairvoyance to foresee the explosion in wireless mobile devices. Nor did Congress anticipate the confusion[237] that would ensue due to the lack of any clear guidance in the ECPA in the form of standards governing law enforcement compelled disclosures for prospective location information.

In contrast to the uncertain, even chaotic, legal landscape that currently burdens the analysis of law enforcement access to location data, clear standards enable all stakeholders to execute their respective responsibilities certain in the knowledge that they are following the law. For prosecutors and agents, this means they can efficiently get access to location information because they won't have to "haggle" over the appropriate standard for access with certain judges. For magistrate judges, clear standards better enable them to ensure that the government follows the law in obtaining access to any location data. Moreover, industry can comply with the law without running

236. *See* Comments of CTIA—The Wireless Association, *supra* note 46, at 16 ("The lack of a consistent legal standard for tracking a user's location has made it difficult for carriers to comply with location demands."); *Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 7 (testimony of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice); *Location Hearing*, *supra* note 19, at 85 (written statement of Judge Stephen Wm. Smith, U.S. Magistrate Judge).

237. *See supra* Part III.

the current risk of incurring liability for inappropriately disclosing customer information to the government.[238]

2. Technology Neutrality

In order for the ECPA to remain a "forward looking statute,"[239] even with respect to the next generation of smartphones, it is critical that law enforcement access standards do not depend on the precision and capabilities of particular location technologies, or with the general state of the industry at the time of drafting. There has been an explosion in the growth of location-based services over the past several years. During that time, the precision of the location information these technologies produce has increased dramatically, such that single cell tower data—particularly where enhanced by some of the 350,000 femtocells deployed around the country[240]—is becoming as accurate as GPS.[241] Indeed, the rapid pace of innovation, driven by market incentives to enhance the accuracy of location-based advertising, suggests that location information will continue to become increasingly precise.

A standard that is dependent on the precision of the location data requested creates an unstable, unworkable situation where, for example, certain magistrate judges feel compelled to examine deployment maps of cell towers or seek expert guidance to determine the precision of the location data produced in a particular district.[242] To foster clear rules that can be applied without undue confusion, ultimately leading to greater stability in the law, Congress should enact law enforcement access standards that are not dependent on the specific precision of location data.

3. Standards Alone Will Not Achieve the Appropriate Balance

Most of the privacy community's location information advocacy to date has focused on a "high" standard for law enforcement access. This focus has led to a stalemate with much of the law enforcement community and has put powerful members of Congress "on guard" to protect law enforcement equities. Regardless of the standard required for law enforcement access to

238. *See generally* Albert Gidari, Jr., *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535 (2007).

239. *See House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 10 (written statement of James X. Dempsey, Vice President of Pub. Policy, Ctr. for Democracy & Tech.).

240. *See* Press Release, Informa Telecoms & Media, *supra* note 27.

241. *See In re 2010 S.D. Tex. Application*, 747 F. Supp. 2d 827, 834 (S.D. Tex. 2010) ("As cellular network technology evolves, the traditional distinction between 'high accuracy' GPS tracking and 'low accuracy' cell site tracking is increasingly obsolete, and will soon be effectively meaningless."); *see also supra* Section II.F.

242. *See supra* Sections III.A.2, III.A.3.

location data, there are some privacy concerns that can only be addressed through post collection process and rules, such as data minimization, subscriber notification, and statistical reporting. A regime of reasonable access standards combined with downstream privacy protections seems to present the best way forward.

4. Insistence on a Single Location Standard Is a "A Foolish Consistency"[243]

As stated in the Introduction, this proposal is not the most privacy protective, the least burdensome to industry, or the most law enforcement friendly. Rather, it is an attempt to eliminate the uncertainty and instability currently plaguing the law and to achieve a balance of equities that is more palatable insofar as it improves the positions of each of these stakeholders in some appreciable way. The process of passing legislation is largely about compromise. As a result, the "right" and politically feasible policy balance may not always create a perfectly "consistent" set of law enforcement access standards or privacy protections, if consistency is to be read as mere verbal or structural symmetry for its own sake.

Some privacy scholars have argued that the law, as a matter of policy, should treat historical and prospective location data the same, specifically calling for a justification for treating them anything other than the same.[244] Such an approach, however, would be a significant departure from existing statutory surveillance law, which has traditionally treated historical (stored) and prospective (real time) information differently, requiring more process when the government compels real time information.[245] Insistence upon a

243. "A foolish consistency is the hobgoblin of little minds, adored by little statesmen and philosophers and divines." Ralph Waldo Emerson, *Self Reliance*, *in* 2 THE COLLECTED WORKS OF RALPH W. EMERSON: ESSAYS: FIRST SERIES 33 (Joseph Slater et al. eds., 1979) (1841).

244. At the 2011 Privacy Law Scholars Conference, co-sponsored by the law schools at the University of California, Berkeley and The George Washington University, the authors workshopped a draft of this Article. Several privacy scholars and members of the privacy community questioned our justification for treating stored location information differently from real time location data, advocating for a standard that would require a warrant for all location data.

245. For example, the government can use a subpoena to obtain stored telephone toll records, *see* 18 U.S.C. § 2703(c)(2) (2010), but must get a Pen/Trap order from a court to obtain the same information in real time, *see id.* § 3121. In order to obtain the content of e-mails in real time, the government must meet higher hurdles of a wiretap "super" warrant, which requires a court to find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," *id.* § 2518(c), in addition to several other "probable cause" requirements, *see id.* § 2518 (a)–(b), (d). On the other hand, the government can get stored e-mail content by meeting the standard Rule 41 "probable cause" showing, or less. *See* § 2703(a)–(b); *see also Location Hearing*, *supra*

standard that is "consistent" in the sense only of being identically applied to this distinction would serve only to polarize the legislative process to the point of collapse. Law enforcement will predictably retreat to one corner in order to demonstrate how a probable cause standard for all location data would unduly limit investigative activities[246] while privacy advocates will just as predictably withdraw support for any legislation that authorizes law enforcement to compel all location information with a unitary standard lower than probable cause. Empathy is lost. Synthesis is precluded. This familiar impasse, which has become the norm in our recent political life, is here the fruit of a foolish consistency that would level a long-held distinction between two categories of data and, in doing so, likely derail a legislative balancing process that could improve the position of all stakeholders when measured against the current state of the law.

As a matter of legislative strategy then, mandating a single standard for the sake of this leveling form of consistency has risks. Such consistency can, of course, cut both ways: it would be equally consistent to allow law enforcement access to all location data with either a probable cause warrant or a D Order. Indeed, consistency for its own sake, argued in either direction, is a reductive, polarizing position that short-circuits any legislative effort to harmonize the competing policy interests of the privacy and law enforcement communities.

B. HOW TO DEFINE LOCATION INFORMATION FOR PURPOSES OF AMENDING THE ECPA

There are many data forms that reveal an individual's location and that law enforcement can compel from third-party providers. These sources include wireless phone carriers and smartphone platform vendors (such as Apple and Google). Location information can also be discerned through transactional records, such as tollbooth, public transport, and credit card records.[247] Law enforcement agencies can also obtain location information directly, without going to third parties, by intercepting wireless phone signals

note 19, at 82 (written statement of Judge Stephen Wm. Smith) (explaining levels of privacy protection given to different surveillance authorities).

246. *See supra* Section IV.B.

247. *See* Ryan Singel, *Feds Warrantlessly Tracking Americans' Credit Cards in Real Time*, WIRED (Dec. 2, 2010), http://www.wired.com/threatlevel/2010/12/realtime/ ("Federal law enforcement agencies have been tracking Americans in real-time using credit cards, loyalty cards and travel reservations without getting a court order, a new document released under a government sunshine request shows. . . . [S]o-called 'Hotwatch' orders allow for real-time tracking of individuals in a criminal investigation via credit card companies, rental car agencies, calling cards, and even grocery store loyalty programs.").

using a Triggerfish, Stingray, or other similar tracking technologies,[248] or by covertly installing a GPS tracking device under a car. While law enforcement's access to these sources of data all raise legitimate privacy concerns, this Article focuses on the compelled disclosure of location information from communications carriers, such as mobile phone services. Congress can, and should, look into other forms of location surveillance, but they remain beyond the scope of this Article. Our proposed standard, directed at third-party communication carriers, begins with the following statutory definitions:

> An "electronic location service" ("ELS") is any service which possesses location information about a customer, subscriber, or user.
>
> "Location information" ("LI") is any information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, or user.[249]
>
> "Historical location information" is location information that existed prior to the issuance of an order.
>
> "Current or prospective location information" is location information that comes into existence after a court order for disclosure of that information is issued.

---

248. *Cell Site Simulators, Triggerfish, Cell Phones* (last updated Feb. 23, 2007), *in* U.S. Dep't of Justice, Response to Freedom of Information Act Request No. 07-4130 re: Mobile Phone Tracking 18 (Aug. 12, 2008), *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (stating that Triggerfish can be deployed "without the user knowing about it, and without involving the cell phone provider"); Julian Sanchez, *FOIA Docs Show Feds Can Lojack Mobiles Without Telco Help*, ARS TECHNICA (Nov. 16, 2008), http://arstechnica.com/tech-policy/news/2008/11/foia-docs-show-feds-can-lojack-mobiles-without-telco-help.ars ("The Justice Department's electronic surveillance manual explicitly suggests that triggerfish may be used to avoid restrictions in statutes like CALEA that bar the use of pen register or trap-and-trace devices—which allow tracking of incoming and outgoing calls from a phone subject to much less stringent evidentiary standards—to gather location data."); *see also* Jennifer Valentino-DeVries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL ST. J. (Sept. 22, 2011), http://on.wsj.com/IhMb7d.

249. "Radio" refers to the radio frequency ("RF") portion of the electromagnetic spectrum, which is "generally defined as that part of the spectrum where electromagnetic waves have frequencies in the range of about 3 kilohertz [3000 hertz] to 300 gigahertz." FED. COMMC'NS COMM'N, BULLETIN NO. 56, QUESTIONS AND ANSWERS ABOUT BIOLOGICAL EFFECTS AND POTENTIAL HAZARDS OF RADIOFREQUENCY ELECTROMAGNETIC FIELDS 2–3 (4th ed., 1999), *available at* http://www.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet56/oet56e4.pdf; *see also Radio*, MERRIAM-WEBSTER DICTIONARY ONLINE, http://www.merriamwebster.com/dictionary/radio (last visited Mar. 19, 2012) (defining radio as "of or relating to electric currents or phenomena (as electromagnetic radiation) of frequencies between about 3000 hertz and 300 gigahertz").

C. A STANDARD FOR LAW ENFORCEMENT COMPELLED DISCLOSURES OF HISTORICAL LOCATION DATA

Our proposed law enforcement access standard for historical location information is built around the current D Order standard with the addition of an element specifically requiring courts to examine whether the scope of the request is reasonable in light of the criminal activity being investigated. We have previously discussed certain examples of scope permutations in investigations[250]—it would be useless to try and define all of them in advance. A discussion of how Congress generally views the scope inquiry could also be developed in legislative history. A court, when applying the standard, will focus the scope of its inquiry on issues raised (and perhaps resolved) by the specific facts presented by the government in its application for a D Order. This standard could be drafted as follows:

> (a) DISCLOSURE UPON COURT ORDER.—Except as provided in paragraph (3), a provider of an electronic location service shall provide historical location information to a governmental entity only if the governmental entity obtains a court order issued by any court of competent jurisdiction establishing—
>
> (1) specific and articulable facts showing that there are reasonable grounds to believe that the location information requested is relevant and material to an ongoing criminal investigation; and
>
> (2) specific and articulable facts showing that a reasonable and sufficient nexus exists between the alleged or suspected criminal activity described in paragraph (1) and the scope of the location data requested.
>
> (3) PERMITTED DISCLOSURES WITHOUT COURT ORDER.—A provider of an electronic location service may disclose historical location information with—
>
> (A) the express consent of the customer, subscriber, or the user of the equipment concerned; or
>
> (B) as otherwise authorized in 18 U.S.C. § 2702(c)(3)–(6).

By maintaining the "relevant and material" language, our standard preserves law enforcement equities while limiting the unnecessary over-collection of historical location information by requiring courts specifically to approve the scope of a request. Moreover, this standard "forces" the government to articulate how the scope of the request is reasonable in light of the particular

250. *See supra* Section III.C.1.

facts and needs of the investigation.[251] We hope that this type of balancing can foster a compromise between privacy advocates and law enforcement insofar as it does not raise the historical data access standard up to probable cause that would unduly limit law enforcement in the early stages of an investigation, but it does require written justification and court approval for the scope of the request.

This standard also maintains the exceptions for disclosure of non-content records already present in the ECPA, including emergencies involving danger of death or serious physical injury.[252] Finally, this proposed language clearly establishes the standard the government must meet before obtaining access to historical location data, a change that benefits all stakeholders.

D. A STANDARD FOR LAW ENFORCEMENT COMPELLED DISCLOSURES OF PROSPECTIVE LOCATION DATA

Our proposed standard for prospective location information requires a probable cause showing. We expand the categories of that showing, however, to accommodate common, legitimate law enforcement uses of prospective location data, including location information pertaining to a person who has committed, is committing, or is about to commit a felony offense or is a victim of that offense.

The DOJ has acknowledged that, as a matter of policy, it already advises prosecutors and agents to obtain a probable cause warrant for GPS or similarly precise location information.[253] Our standard not only codifies the DOJ's existing practice regarding GPS and similarly precise location data but also requires a probable cause showing (based on the expanded categories) for all prospective location data. Insofar as single cell site data can now be as precise as GPS location information—and such precision will only continue to increase over time—drawing distinctions in the law based upon data precision is no longer logical or workable.[254]

---

251. Indeed, in Stephanie's experience as a federal prosecutor, when a standard calls for this type of explanation, prosecutors and agents are much more likely to tailor applications narrowly at the outset, in anticipation of court scrutiny.

252. One of the current ECPA exceptions, 18 U.S.C. § 2702(c)(6) (2010), puts no limits on providers sharing non-content information with third parties who are not law enforcement. In recent testimony, the DOJ has suggested that it may be appropriate for Congress to consider restricting disclosures of personal information by service providers. *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 10 (testimony of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice). Insofar as this Article focuses on law enforcement access issues, it is beyond the scope of this Article to address this issue.

253. *See Senate Judiciary 2011 ECPA Hearing*, *supra* note 7, at 7 (testimony of James A. Baker).

254. *See supra* Sections III.A.1, III.B.1, III.C.1, IV.B; *see also Location Hearing*, *supra* note 19, at 85 (written statement of Judge Stephen Wm. Smith).

With the expansion of the categories of probable cause, we have once again attempted to accommodate law enforcement investigative needs[255] in order to foster a compromise between law enforcement and privacy advocates. This standard could be drafted as follows:

> (1) DISCLOSURE UPON COURT ORDER FOR A PERIOD NOT TO EXCEED 30 DAYS.—Except as provided in paragraph (2), a provider of an electronic location service shall provide a governmental entity current or prospective location information about a customer, subscriber, or user only if the governmental entity obtains a court order from any court of competent jurisdiction issued upon a finding that there is probable cause to believe that—
>
> (A) the information sought is evidence of a crime; or
>
> (B) a person is committing, has committed, or is about to commit a felony offense or is a victim of that offense; and the location information sought to be obtained concerns the location of the person believed to have committed, be committing, or be about to commit that offense or a victim of that offense.
>
> (2) PERMITTED DISCLOSURES WITHOUT COURT ORDER.—A provider of an electronic location service may provide the information described in paragraph (1)—
>
> (A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;
>
> (B) with the express consent of the customer, subscriber, or the user of the equipment concerned; or
>
> (C) as otherwise authorized in 18 U.S.C. § 2702(c)(3)–(6).
>
> (3) DEFINITION.—The term "public safety answering point" means a facility that has been designated to receive emergency calls and route them to emergency service personnel.
>
> (4) EXTENSIONS.—Extensions of such an order may be granted for up to 30 days upon a probable cause showing as defined in sections (A)–(B) of paragraph (1) of this provision.

This statutory language is not from the ECPA reform hearings of 2010–2011.[256] Rather, it is adopted from a bill, entitled the "Electronic Communications Privacy Act of 2000," reported out favorably by a

255. *See supra* Section III.C.

256. *See* discussion *supra* Parts I, IV.

Republican-controlled House Judiciary Committee. The bill never became law, but it applied the "expanded" probable cause standard to prospective location information.[257] These expanded probable cause standards address situations where, for example, law enforcement may have probable cause to believe someone has committed a crime yet the suspect's current or prospective location information may not itself be evidence of a crime.[258]

Consistent with other real-time surveillance authorities like Pen/Trap and the Wiretap Act, our proposal affords prospective location information a higher degree of privacy protection than that given to previously stored information.[259] Also mirroring the Wiretap Act,[260] our proposal places a time limit of thirty days for each individual order, without preventing the government from returning to a court for an extension. This standard also includes specific exceptions to allow for the operation of the E-911 system[261] while incorporating all of the exceptions for non-content information already present in the ECPA. Finally, this proposed language clearly establishes a standard the government must meet before getting access to prospective location data, a change that again benefits all stakeholders.

E. POST ACCESS RULES AND "DOWNSTREAM" PRIVACY PROTECTIONS

It is obviously important for Congress to select the right legal standard required for law enforcement to obtain location data. Equally important to an overall privacy framework, however, are rules regarding the retention of the data once it is acquired, notice to individuals whose information has been acquired by law enforcement, and reporting requirements to Congress.[262] Indeed, such "downstream" protections can offset any over-collection of information by law enforcement during the course of an investigation. This Section proposes three specific methods to protect privacy following the

257. *See* H.R. 5018, 106th Cong. § 6(a) (2000).

258. *See supra* Section III.C.2.

259. *See* discussion *supra* note 245 and accompanying text.

260. 18 U.S.C. § 2518(5) (2010).

261. *Location Hearing*, *supra* note 19, at 36 (statement of Michael Amarosa, Sr. Vice President for Public Affairs, TruePosition Inc.) (describing the FCC E-911 requirement).

262. *See* Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law,* FUTURE CONST. (Brookings Inst., Washington, D.C.), Apr. 19, 2011, *available at* http://www.brookings.edu/papers/2011/0419_surveillance_laws_kerr.aspx ("[T]he law should still regulate the collection of evidence. But surveillance law shouldn't end there. The shift to computerization requires renewed attention on regulating the use and disclosure of information, not just its collection.").

disclosure of location information to law enforcement: minimization, notification, and congressional oversight through statistical reporting.[263]

1. Minimization

Given the large amount of data that law enforcement agencies now obtain via location requests and the number of innocent people whose information may be obtained through community of interest requests or requests associated with a specific place, we believe that minimization rules can and should play a role in limiting the privacy harms associated with such data collection. These minimization rules would focus on removing irrelevant location data from law enforcement databases at a time appropriate to the particular investigation or case. Minimization requirements are not a new idea. They already play a privacy protective role in several other surveillance statutes, including the Wiretap Act,[264] the USA PATRIOT Improvement and Reauthorization Act of 2005 ("PATRIOT Act"),[265] and the Foreign Intelligence Surveillance Act ("FISA").[266]

Although Congress has frequently enacted minimization requirements, it has never legislated the specific details of how such minimization would work with respect to particular surveillance authorities or investigations. In both the Wiretap Act and FISA, government lawyers submit minimization protocols as part of their applications, which are then approved by a judge and included in the court order. Likewise, in the PATRIOT Act, Congress directed the DOJ to adopt specific minimization procedures for records

263. There are other types of downstream privacy protections that could and perhaps should eventually be included in a privacy framework—e.g., the unsealing of court orders with appropriate redactions at a time when such unsealing would no longer jeopardize an investigation or place individuals involved in it at risk. *See, e.g.*, Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177 (2009) (arguing that the overabundant, indefinite sealing of certain types of judicial orders undermines the legitimacy of those decisions). For the purpose of making good policy, unsealing, whether after a specified period or after specific conditions have been met, could facilitate greater transparency and provide Congress with better information about how the government uses and courts apply surveillance authorities. Notwithstanding the potential utility of such a policy, however, we believe that the unsealing of court records raises serious security and privacy issues that require a complex and lengthy analysis that is beyond both the scope of ECPA reform and this Article.

264. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 for the first time authorized law enforcement personnel to monitor private telephone conversations. Pub. L. No. 90-351, tit. III, 92 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2511–2520 (2010)). The Act also provided strict guidelines and limitations on the use of wiretaps as a barrier to government infringement of individual privacy. One of the protections included by Congress was the minimization requirement of 18 U.S.C. § 2518(5).

265. 50 U.S.C. § 1861(g) (2009).

266. *Id.* § 1804(a)(5).

obtained pursuant to Section 215 orders. Section 215 is a national security collection authority that allows the government to obtain both content and non-content information.[267]

As such, we propose that Congress should require the DOJ, in consultation with State Attorneys General, to develop rules and procedures for the minimization of location information. Such rules would be intended to prevent the retention of information that is not relevant to reasonable law enforcement purposes. Statutory language could be drafted as follows:

> The Attorney General, in consultation with State Attorneys General, shall adopt specific minimization procedures governing the retention and dissemination by governmental entities of location information received in response to an order under this section.
>
> In this section, the term "minimization procedures" means specific procedures, reasonably designed in light of the form and purpose of an order for the production of location information, to minimize the retention and prohibit the dissemination of non-publicly available location information concerning non-consenting persons, consistent with the need of law enforcement to obtain, retain, produce, and disseminate information that: 1) is evidence of a crime; or 2) concerns the location of a person who is committing, has committed, is about to commit, or is a victim of a felony offense; or 3) is otherwise relevant and material to an ongoing criminal investigation and to be retained or disseminated for law enforcement purposes.

This language gives the Attorney General, in conjunction with the State Attorneys General, the flexibility and discretion to design minimization rules and procedures consistent with law enforcement needs while minimizing the retention and dissemination of location data that is not or is no longer relevant to legitimate law enforcement purposes.

2. Notification

Covert surveillance methods are investigative tools that by their very nature invade the privacy of those targeted and are, as history has shown, prone to abuse.[268] To ensure these surveillance powers are restricted to

267. Section 1861 of Title 50, commonly referred to as "Section 215 Business Records," permits the government to obtain, with a FISA court order, any "tangible thing" for certain types of national security investigations. Such Section 215 minimization procedures were intended to minimize the retention and prohibit the dissemination of non-publicly available information concerning United States persons consistent with national security interests. *See* § 1861(g).

268. *See* Julian Sanchez, *Wiretapping's True Danger*, L.A. TIMES (Mar. 16, 2008), http://articles.latimes.com/2008/mar/16/opinion/op-sanchez16 ("Without meaningful oversight, presidents and intelligence agencies can—and repeatedly have—abused their surveillance

legitimate law enforcement investigative needs, surveillance of innocent persons should be limited whenever possible and, whenever employed, it should not remain secret indefinitely. Such transparency facilitates social and congressional oversight of government use of surveillance techniques: individuals who may have been inappropriately or illegally monitored are provided with information and resulting incentives that may motivate them to pursue personal remedies, such as placing facts about the surveillance in the public record. Indeed, a disclosure mechanism that will raise public awareness of, and stimulate public discourse about, the scope and frequency of government surveillance activities may serve as an important deterrent to gratuitous use or abuse of these powers.

In both the Wiretap Act and the Stored Communications Act, Congress created mandatory notice requirements that guarantee that subjects of some forms of law enforcement surveillance would be told that their communications have been intercepted or accessed.[269] Such notice provisions act as an important privacy protection that particularly benefits those who are subjects of surveillance but never charged with a crime. While those who are eventually arrested and charged might otherwise learn that they have been the target of surveillance (through the disclosure of search warrants, affidavits, and other documents), those who are not charged would never know about their surveillance histories were it not for the existence of notice requirements in existing surveillance laws.

We propose a similar notice requirement for those individuals whose location information is obtained by law enforcement agencies. This requirement will apply to those individuals targeted in location orders, as well

authority to spy on political enemies and dissenters. . . . [A] thorough congressional investigation headed by Sen. Frank Church (D-Idaho) revealed that for decades, intelligence analysts—and the presidents they served—had spied on the letters and phone conversations of union chiefs, civil rights leaders, journalists, antiwar activists, lobbyists, members of Congress, Supreme Court justices—even Eleanor Roosevelt and the Rev. Martin Luther King Jr. The Church Committee reports painstakingly documented how the information obtained was often 'collected and disseminated in order to serve the purely political interests of an intelligence agency or the administration, and to influence social policy and political action.' ").

269. *See* 18 U.S.C. § 2518(8)(d) (Wiretap Act notifications) and §§ 2703(b)(1)(B), 2705 (ECPA notifications). ECPA notifications only apply to the disclosure of content (not non-content) and then only when a § 2703(d) order or subpoena is used to compel content. If using a Rule 41 warrant to compel content, at least one court held that the government only has to notify the service provider, not the customer or subscriber. *In re* Application for Warrant for E-mail Account [redacted]@gmail.com Maintained on Computer Servers Operated by Google, Inc., Headquartered at 1600 Amphitheater Parkway, Mountain View, CA, Mag. No. 10-291-M-01 (D.D.C. Nov. 1, 2010) (Lamberth, J.), *available at* http://www.dcd.uscourts.gov/dcd/sites/dcd/files/mag10-291.pdf.

as innocent individuals whose information may be obtained as part of disclosures associated with specific places or community of interest requests. In addition to facilitating transparency and providing notice to impacted individuals, this requirement will, similar to existing compensation requirements,[270] discourage law enforcement agencies from making unnecessary requests for large amounts of data,[271] as the cost of notifying 200 people will presumably be greater than that of notifying only twenty. This requirement could be drafted as follows:

> (a) NOTIFICATION.—
>
> > (1) Within 90 days after the disclosure of historical location information, or the expiration of an order authorizing prospective location information, the governmental entity shall serve upon, or deliver by appropriate means,[272] the customer, subscriber, or user whose location was disclosed with notice that—
> >
> > > (A) states with reasonable specificity the nature of the law enforcement inquiry; and
> > >
> > > (B) informs such customer, subscriber, or user that their location information was supplied to that governmental authority, and the date on which such disclosure was made.
> >
> > (2) Extensions of the delay of notification of up to 90 days each shall be granted by the court upon application by a governmental entity if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (3) of this subsection.
> >
> > (3) An adverse result for the purposes of paragraph (2) of this subsection is—

---

270. *See House Judiciary 2010 ECPA Reform Hearing*, *supra* note 18, at 32 (written statement of Albert Gidari, Perkins Coie LLP) ("When records are 'free,' such as with phone records, law enforcement over-consumes with abandon. . . . But when service providers charge for extracting data, such as log file searches, law enforcement requests are more tailored.").

271. William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1275 (1999) ("[I]f you tax a given kind of [law enforcement] behavior, you will probably see less of it.").

272. Due to the widespread popularity of prepaid phones, many communications carriers do not have a name or address on file for large numbers of their customers. As a result, it would not be possible for the carriers to notify these customers via U.S. mail (something required for surveillance of internet communications content performed under 18 U.S.C. § 2705(a)(5)). The use of the term "appropriate means" is designed to enable companies to notify their customers via a communication medium that is appropriate to the service they offer, and the contact information they have on file. This could include, for example, email, or mobile text message ("SMS").

> (A) endangering the life or physical safety of an individual;
>
> (B) flight from prosecution;
>
> (C) destruction of or tampering with evidence;
>
> (D) intimidation of potential witnesses; or
>
> (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.
>
> (b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section [*x*] may apply to a court for an order commanding a provider of an electronic location service to whom a court order issued under section [*x*] is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the court order will result in—
>
> (1) endangering the life or physical safety of an individual;
>
> (2) flight from prosecution;
>
> (3) destruction of or tampering with evidence;
>
> (4) intimidation of potential witnesses; or
>
> (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

This section requires the law enforcement agency to notify all persons whose location information it obtains within ninety days after either the disclosure of historical data or the end of prospective surveillance. Individuals shall be notified via "appropriate" means, which could be a series of text messages, an email, or a letter, depending on the contact information known to law enforcement. As with other notification statutes, the proposed section also permits the government to seek further delay of notice with cause, as well as prohibit a location provider from telling a target that her location information has been disclosed. When notifying innocent third parties that their location information was disclosed (incidentally) as part of a "broad" authorization, the governmental entity making the notification should consider language that communicates the benign nature of the disclosure.

3. Surveillance Statistics

When Congress created both the wiretap and pen register/trap and trace interception statutes, it mandated the annual publication of aggregate

statistical reports[273] that were "intended to form the basis for a public evaluation of [the statute's] operation [and] will assure the community that the system of court-ordered electronic surveillance . . . is properly administered."[274] Since at least 1998, the Administrative Office of the United States Courts ("AO") has made copies of these reports available to the general public via its website.[275] The public release of the annual report usually leads to media coverage highlighting the increased use of wiretaps.[276]

These statistics also provide a rich source of information for scholars wishing to study and report on the ever-increasing use of electronic surveillance.[277] By comparing these reports, scholars have been able to observe several notable surveillance trends. These include that the majority of wiretaps are for drug crimes;[278] that courts rarely, if ever, refuse wiretap applications;[279] that the vast majority of wiretaps target mobile phones;[280] and the ever-growing use of wiretaps by state law enforcement agencies.[281]

---

273. *See supra* note 171.

274. S. REP. NO. 90-1097, at 69 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185, *and available at* 1968 WL 4956, at *2185.

275. *See, e.g.*, ADMIN. OFFICE OF THE U.S. COURTS, 1997 WIRETAP REPORT (1998), http://web.archive.org/web/19981206135425/www.uscourts.gov/wiretap/contents.html.

276. *See, e.g.*, *National News Briefs; Record Total of Wiretaps Was Approved by Courts*, N.Y. TIMES (May 10, 1998), http://nyti.ms/IhNhQj; Susan Stellin, *Compressed Data; Who's Watching? No, Who's Listening In?*, N.Y. TIMES (June 3, 2002), http://nyti.ms/IhNp2d; Ryan Singel, *Police Wiretapping Jumps 26 Percent*, WIRED (Apr. 30, 2010), http://www.wired.com/threatlevel/2010/04/wiretapping/.

277. *See Cloud Based Computing Hearing*, *supra* note 165, at 130 (oral answer from Fred Cate, Prof. and Director, Ctr. for Applied Cybersecurity Research, Ind. Univ., to Chairman Nadler) ("[Surveillance] statistics gives Congress a sound empirical basis on which to evaluate how its laws are being used and whether they need to be changed. It also provides that same information for people such as those of us gathered at this table when making recommendations to Congress. And it provides information to the public and the press so that they know how those laws are being used and to what effect."); *see also* Soghoian, *supra* note 170.

278. Soghoian, *supra* note 170, at 9 ("[M]ore than 86 percent of the 2306 wiretap orders obtained [in 2009] by federal and state law enforcement agencies were sought in narcotics investigations.").

279. *See id.* at 6–7 ("Between 1987 and 2009, law enforcement agencies requested over 30,000 wiretap orders. . . . During the more than 20 years for which public data exists, requests for wiretap orders have been rejected just 7 times, twice in 1998, once in 1996, twice in 1998, once in 2002 and once in 2005.").

280. *See id.* at 7 ("96 percent (2,276 wiretaps) of all authorized wiretap for 2009 are for portable devices.").

281. *See id.* at 12 ("Over the last decade, the use of electronic surveillance orders has increased nationwide, although this is largely due to a massive increase in use by the states . . . . [California and New York] are now responsible for a combined 58 percent of all state wiretap orders.").

While much is known about the scale and use of wiretaps and, to a lesser extent, Pen/Trap surveillance, law enforcement requests for location information are largely a "known unknown."[282] Wireless companies and their representatives have provided, at best, a partial picture whose details emerge only through Freedom of Information Act requests and other investigative reporting techniques by privacy advocates.[283] That picture is not sufficiently clear to guide Congress regarding the use of this surveillance technique.[284] To remedy this deficiency, we propose a specific reporting requirement that will enable Congress to know as much about the state of location surveillance as it currently knows about wiretaps and would, as Senator Patrick Leahy has described, provide a "far more reliable basis than anecdotal evidence on which to assess law enforcement needs and make sensible policy in this area."[285] This standard could be drafted as follows:

> (a) GENERAL RULEMAKING AUTHORITY FOR REPORTS UNDER THIS SECTION.—The Director of the Administrative Office of the United States Courts may make rules regarding the content and form of the reports required under this section.
>
> (b) REPORTS CONCERNING DISCLOSURES.—
>
> (1) TO ADMINISTRATIVE OFFICE.—Not later than 30 days after the issuance or denial of an order under this chapter compelling the disclosure of location information, the issuing or denying judge shall report to the Administrative Office of the United States Courts—
>
> (A) the fact that an order was applied for;
>
> (B) the type of order applied for;
>
> (C) whether the order was granted as applied for, was modified, or was denied;
>
> (D) whether the court also granted delayed notice and the number of times such delay was granted;
>
> (E) the offense specified in the order or application, or extension of an order;

---

282. News Transcript, U.S. Dep't of Defense, DoD News Briefing—Secretary Rumsfeld and Gen. Myers (Feb. 12, 2002), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636 ("[T]here are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know."); *see also supra* Part I (discussing details about what is known regarding the scale of location surveillance).

283. *See generally* Soghoian, *supra* note 170.

284. *Id.*

285. 145 CONG. REC. 31,311 (1999) (statement of Sen. Leahy).

(F) the identity, including district where applicable, of the applying investigative or law enforcement agency making the application and the person authorizing the application; and

(G) the type of information or records sought in the order.

(2) TO CONGRESS.—In April of each year the Director of the Administrative Office of the United States Courts shall report to Congress with respect to the preceding calendar year—

(A) the overall total number of each of the events described in the subparagraphs of paragraph (1), regarding applications reported to that Office; and

(B) a summary and analysis of the data described in paragraph (1).

(c) PROVIDER REPORTING REQUIREMENTS.—

(1) TO ADMINISTRATIVE OFFICE.—Except as provided in paragraph (2), in January of each year each provider of an electronic location service shall report with respect to the preceding calendar year to the Administrative Office of the United States Courts—

(A) the number of legal demands and emergency requests received from Federal law enforcement agencies during the preceding calendar year for location information;

(B) the number of legal demands and emergency requests received from State, local, and tribal law enforcement agencies during the preceding calendar for location information; and

(C) the number of accounts about which location information was disclosed, specifying the numbers disclosed pursuant to legal demand and the numbers disclosed voluntarily, to Federal, State, local, or tribal law enforcement agencies.

(2) EXCEPTIONS.—The requirement of paragraph (1) does not apply to a provider of an electronic location service that, during the reporting period—

(A) received fewer than 50 requests combined from law enforcement agencies; or

(B) disclosed account information concerning fewer than 100 subscribers, customers, or other users; or

(C) had fewer than 100,000 total customers or subscribers at the end of the calendar year.[286]

286. The purpose of these statistics is to provide Congress, scholars, and the general public with information necessary to determine the scale of surveillance and to observe

(3) COMPENSATION.—The Director of the Administrative Office of the United States Courts shall provide reasonable compensation to a provider for the costs of compiling a report required under this subsection.[287]

(4) CONFIDENTIALITY OF IDENTITY OF SERVICE PROVIDERS.—The Director of the Administrative Office of the United States Courts shall establish procedures to prevent the release to the public of the identity of service providers with respect to disclosures they make under this subsection.[288]

(5) TO CONGRESS.—In April of each year, the Director of the Administrative Office of the United States Courts shall report to Congress with respect to the preceding calendar year—

(A) the total numbers of legal demands and of disclosures required to be reported under paragraph (1); and

(B) a summary and analysis of the information required to be reported by paragraph (1), but without disclosing the identity of any service

general trends. Information from small providers who receive just a handful of requests per year will not significantly aid in the ability to observe such trends, in comparison to the tens of thousands of requests received by large providers. Furthermore, this notice requirement, while modest, could still be quite burdensome for a small provider. It is for this reason that we have opted to exempt such providers from the statistical reporting requirements.

287. As a general rule, companies are not in favor of regulations that are costly to comply with. Although we do not believe that the cost of compiling and submitting these reports will be exceedingly expensive (particularly given that Google already provides some data voluntarily), we have included a compensation provision to avoid giving companies a reason to lobby against it. We believe that the data that will be made public as a result of this provision is worth the modest cost to the taxpayer.

288. Although most large internet and telecommunications companies that handle user data receive both compulsory and voluntary location data requests from the government, few like to discuss the topic publicly. As such, many companies might vigorously oppose this statistical reporting requirement if it would mean that their names would be associated with the data that eventually becomes published. In order to respond to companies' concerns, this provision has been drafted to ensure that identities of the companies will remain confidential: only aggregate statistics will be published. In March 2010, Microsoft Associate General Counsel Mike Hintze told a reporter at *Wired* that the reason Microsoft does not publish statistical data regarding the number of legal requests the company receives for customer information is due to the fear of negative publicity. "We would like to see more transparency across the industry," Hintze said. "But no one company wants to stick its head up to talk about numbers." Ryan Singel, *Google, Microsoft Push Feds To Fix Privacy Laws*, WIRED (Mar. 30, 2010), http://www.wired.com/threatlevel/2010/03/google-microsoft-ecpa/; *see also* Letter from Michael T. Gershberg, Counsel to Yahoo! Inc, to William Bordley, FOIPA Officer, U.S. Marshals Serv. 9 (Sept. 15, 2009), *available at* http://cryptome.org/yahoo-price-list-letter.pdf ("[Surveillance pricing] information, if disclosed, would be used to 'shame' Yahoo! and other companies—and to 'shock' their customers. Therefore, release of Yahoo!'s information is reasonably likely to lead to impairment of its reputation for protection of user privacy and security, which is a competitive disadvantage for technology companies.").

> provider with respect to the disclosures to law enforcement that service provider made.

This section creates a new statistical surveillance report for Congress that documents the issuance of orders compelling the disclosure of location information. The AO[289] will compile the annual report based on information submitted to it by judges who have issued orders in response to government applications to compel location information. The AO will then submit the compiled information in a report to Congress. This section also requires providers of an electronic location service (other than those falling below a *de minimis* threshold) to submit annual reports regarding the number of compelled and voluntary disclosures of location information they have made to the AO.[290] The AO will then compile the data collected, produce a statistical summary containing no reference to the names of individual providers, and submit the information in a report to Congress.

VII. CONCLUSION

The use of location information by law enforcement agencies is common and is becoming more so as technology improves and produces more accurate and precise location data. The legal mystery surrounding the proper law enforcement access standard for prospective location data remains unsolved and has created, along with conflicting rulings over the appropriate law enforcement access standard for both prospective and historical location data, a messy, inconsistent legal landscape where even judges in the same district may require law enforcement to meet different standards before authorizing law enforcement to compel location data. As courts struggle with these intertwined technology, privacy, and legal issues, some judges are expressing concern over the scope of the harms, from specific and personal to general and social, presented by unfettered government collection and use of location data.

---

289. The AO is the preferred entity to manage and execute this task because it is an objective, neutral organization and because it has historically produced the annual Wiretap Report (part of the Omnibus Crime Control and Safe Streets Act of 1968) in an accurate, timely manner. *See* 145 CONG. REC. 31,311 (1999) (statement of Sen. Leahy) ("The AO has done an excellent job of preparing the wiretap reports."). Placing the reporting burden with the AO also prevents law enforcement from complaining that the reporting requirements are turning "crimefighters into bookkeepers." *House Judiciary 2000 ECPA Hearing*, *supra* note 175, at 39 (statement of Kevin DiGregory, Deputy Assoc. Attorney Gen., Dep't of Justice).

290. The AO is only capable of compiling information on court orders for location information. Statistical data for voluntary disclosures made in emergencies can only come from the providers or law enforcement, and so we have opted to place this burden on the providers, who are then compensated for their trouble.

This Article proposes model law enforcement access standards and downstream privacy protections for location information. This proposal attempts to (1) articulate clear rules for courts to apply and law enforcement agents and industry to follow; and (2) strike a reasonable balance among the interests of law enforcement, privacy, and industry. We believe that our location information framework could form a solid basis for legislation because, among other things, when measured against the current state of the law, it improves the position of all stakeholders appreciably. Industry gains clear rules to follow and is not overly burdened or exposed by reporting requirements. Law enforcement gains clear rules to follow that will not unduly limit their investigative activities, especially in light of certain existing policies voluntarily adopted by the DOJ. Indeed, law enforcement's ability to acquire prospective location information to find individuals who have committed, are committing, or are about to commit a crime, when the location information itself is not evidence of a crime, is arguably improved by these proposed access standards. Moreover, law enforcement participation in a system that features tighter standards for initial access, as well as increased downstream privacy protections like minimization and notice, will promote increased public trust in the integrity of the system and a corresponding increase in law enforcement's own credibility.

While many privacy advocates have lobbied for a probable cause standard for all law enforcement access to location data, we have illustrated that this is not a realistic legislative goal in the current political climate or any immediately foreseeable one. Law enforcement will successfully argue that such a standard will unduly limit its investigative activities, including the ability to exclude someone from an investigation and spare her any unnecessary further inquiry into her personal life. Our proposal, however, offers privacy advocates clear rules that improve upon the current D Order standard and ensures that a probable cause standard will govern all law enforcement compelled disclosures of prospective cell phone location data. Moreover, this privacy framework offers privacy advocates a policy more protective than any threshold access standard alone can provide: downstream privacy protections that, among other things, ensure greater transparency and congressional oversight and minimize government authorities' retention of location data. As a legislative strategy, then, we submit that privacy advocates will stand on much firmer ground in supporting access standards aimed at a reasonable, legitimate balancing of stakeholder equities that also include downstream privacy protections. While privacy advocates can continue to fight for higher access standards for all location data in the courts, their constituents will not benefit from valuable downstream protections unless Congress includes them as part of reasonable, palatable ECPA legislative

reform. Our solution follows the suggestions of some jurists who have considered the potential social harms posed by location-based technologies and services: that Congress may be best suited to address these issues. We agree and offer the foregoing proposal as a strong initial step in that direction.[291]

291. During the writing of this Article, three bills in the 112th Congress were introduced proposing new law enforcement access standards for location data. *See* S. 1011, 112th Cong. (2011); S. 1212, 112th Cong. (2011); and H.R. 2168, 112th Cong. (2011). None of these bills currently contain downstream privacy protections. Two of the bills, S. 1212 and H.R. 2168, require a Rule 41 "probable cause" standard for all law enforcement compelled disclosures of location data, including the use of GPS tracking devices placed on cars. While S. 1011 allows law enforcement to compel historical location data with a D Order, there is no scope element addressing whether there is a sufficient nexus between the alleged or suspected criminal activity and the scope of the location data requested. *See supra* Sections III.C.1, III.C.2. S. 1011, like the two other bills, requires a Rule 41 "probable cause" showing for law enforcement to compel prospective data (including the use of GPS tracking devices) but similarly does not take into account the "probable cause of what" problem that may inhibit law enforcement from acquiring the current or prospective location of a subject who, for example, has committed a past crime when the subject's current or prospective location is not itself evidence of a crime.