32:3 BERKELEY TECHNOLOGY LAW JOURNAL

2017

Pages

1027

to

1300

Berkeley Technology Law Journal

Volume 32, Number 3

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 32 NUMBER 3 2017

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., 20th ed. 2015). Please cite this issue of the *Berkeley Technology Law Journal* as 32 BERKELEY TECH. L.J. ___ (2017).

BTLJ ONLINE

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

INFORMATION FOR AUTHORS

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 Submissions may include previously unpublished articles, essays, book reviews, case notes, or comments concerning any aspect of the relationship between technology and the law.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

Format. Submissions are accepted in electronic format through the 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., 20th ed. 2015).

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

DONORS

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

Partners

COOLEY LLP

FENWICK & WEST LLP

HOGAN LOVELLS

ORRICK, HERRINGTON & SUTCLIFFE LLP

WHITE & CASE LLP

Benefactors

FISH & RICHARDSON P.C.

COVINGTON & BURLING LLP

KASOWITZ BENSON TORRES & FRIEDMAN LLP

WEIL, GOTSHAL & MANGES LLP

KIRKLAND & ELLIS LLP

SIDLEY AUSTIN LLP

LATHAM & WATKINS LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

MCDERMOTT WILL & EMERY

WILSON SONSINI GOODRICH & ROSATI

MORRISON & FOERSTER LLP

WINSTON & STRAWN LLP

Corporate Benefactors

BLOOMBERG LAW

FINJAN CYBERSECURITY

FUTURE OF PRIVACY FORUM

GOOGLE, INC.

INFLEXION POINT

INTEL

HEWLETT FOUNDATION, THROUGH THE CENTER FOR LONG-TERM CYBERSECURITY

LITINOMICS

MICROSOFT CORPORATION

NOKIA

PALANTIR

THE WALT DISNEY COMPANY

Members

BAKER BOTTS LLP

BAKER & MCKENZIE LLP

DESMARAIS LLP

DURIE TANGRI LLP

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP

GILLIN JACOBSON ELLIS LARSEN & LUCEY

GTC LAW GROUP LLP & AFFILIATES

HAYNES AND BOONE, LLP

IRELL & MANELLA LLP

KEKER & VAN NEST LLP

KILPATRICK TOWNSEND & STOCKTON LLP

KNOBBE MARTENS OLSON & BEAR LLP

PAUL HASTINGS LLP

ROPES & GRAY LLP

SIMPSON THACHER & BARTLETT LLP

TURNER BOYD LLP

VAN PELT, YI & JAMES LLP

WEAVER AUSTIN VILLENEUVE & SAMPSON, LLP

BOARD OF EDITORS 2016–2017

Executive Committee

Editor-in-Chief
MAX DE LA CAL

Managing Editor
CHRIS YANDEL

Senior Articles Editors
WAQAS AKMAL
CHRISTIAN CHESSMAN
BILAL MALIK

Senior Executive Editor
ERICA FISHER

Senior Scholarship Editor
MARK JOSEPH

Senior Annual Review Editors
JESSICA BRODSKY
CASSY HAVENS
JON TANAKA

Senior Online Content Editor
LIDA RAMSEY

Editorial Board

Commentaries Editors
TIFFANY LEUNG

Production Editors
KRISTOFER HATCH
DUSTIN VANDENBERG
CHELSEA MORI
LOUISE DECOPPET

Technical Editors
AYN SU WOODWARD
RICHARD SIMS

Annual Review Editors
BARCLAY OUDERSLUYS
JOYCE LI

Notes & Comments Editors
STEPHEN CHAO
KELSEA CARLSON

Symposium Editors
VANESSA ING
MICHELLE PARK

Submissions Editors
KEVIN CHIU
BRITTANY BRUNS

Online Content Editor
KATE BRIDGE

Web & Technology Editors
JOE CRAIG
TED KANG

Member Relations Editor
TAMARA WIESEBRON

Alumni Relations Editor
JESSICA ANNIS

External Relations Editor
GAVIN MOLER

Articles Editors

ALICE CHI
BRIAN HALL
DARIUS DEHGHAN
ETHAN FRIEDMAN
FAITH SHAPIRO
JEREMY ISARD
MEGHAN FENZEL
MEI LIU
NOA DREYMANN
TIM HSIEH
ROBERT OLSEN
MY THAN
STEPHEN WILSON
JONATHON MADDERN
BRANDON OREWYLER

MEMBERSHIP

Vol. 32 No. 3

Associate Editors

BLAKE ANDERSON
ALEX BARATA
ANTHONY BEDEL
KATIE BURKHART
EDUARDO CORDOVA SAKIKI
KATHERINE CUMMINGS
AMIT ELAZARI
BRITTANY JOHNSON
YARDEN KAKON
LAURA KELLY
ROMAN KRUPENIN
KURT KURZENHAUSER
ANNIE LEE
NIR MAOZ
CHARLES MILLER
ANDREW NGUYEN
ALYSE RITVO
MERCEDES SEGOVIANO GUILARTE
ORNAN STEINBERG
ERICA SUN
SADAF TABATABAI
CHANTE WESTMORELAND

Members

LAUREN AZEKA
DAVID BEHREND
MARIA BELTRAN
CHRISTOPHER BROWN
NIKY BUKOVCAN
ALEXIS CALIGIURI
DEREK CHIPMAN
ERIC CHUANG
RACHEL DALLAL
TRENTON DAVIS
DARIUS DEHGHAN
BROOKES DEGEN
JORDAN FRABONI
ANDREW GLIDDEN
ADAM GREENE
MARK JAYCOX
PATRICK JOHNSON
JIMMY JOHNSTON
AARON LEE
DINA LJEKPERIC
BLAKE MEREDITH
BIHTER OZEDIRNE
REID PAOLETTA
RAJAN PATEL
ANDREW SCHMIDT
NATHAN THEOBALD
AAMIR VIRANI
PAUL WAGNER
KEXI WANG
JIHYUN YU
EMRE YUZAK

BTLJ ADVISORY BOARD

BERKELEY CENTER FOR LAW & TECHNOLOGY 2016–2017

Executive Director

JIM DEMPSEY

Faculty Directors

KENNETH A. BAMBERGER PETER S. MENELL PAMELA SAMUELSON

CATHERINE CRUMP ROBERT P. MERGES PAUL SCHWARTZ

CHRIS HOOFNAGLE DEIRDRE MULLIGAN JENNIFER URBAN

CATHERINE FISK SONIA KATYAL TEJAS NARECHANIA

ANDREA ROTH MOLLY VAN HOUWELING

Fellows

KATHRYN HASHIMOTO GRAHAM RAVDIN

Staff Directors

JANN DUDLEY RICHARD FISK

IRYS SCHENKER CLAIRE TRIAS

FTC 2.0: KEEPING PACE WITH ONLINE PLATFORMS

Terrell McSweeny[†]

ABSTRACT

As the nation's top consumer protection agency, the Federal Trade Commission (FTC) has played a key role in the regulation of online platforms. This essay, originally delivered as the David Nelson Keynote, reviews how the FTC has adapted its century-old consumer protection and antitrust mandate to the digital world and what it must do to keep pace with increasingly powerful platforms. It examines the benefits and drawbacks of relying solely on the FTC's harm-focused, enforcement-based framework to address increasingly powerful technology and proposes updates to the FTC that will help it continue to be an effective consumer protection enforcement agency for the digital age.

DOI: https://doi.org/10.15779/Z38736M23N

† The views expressed herein are Commissioner McSweeny's own and do not represent those of the Federal Trade Commission or any other Commissioner. Commissioner McSweeny thanks her attorney advisor, Christine DeLorme, for her extensive contribution to this Essay.

TABLE OF CONTENTS

I. INTRODUCTION

Online platforms pose a complex challenge for policymakers. How and when platforms are regulated raises profound questions about how we organize ourselves in a digital economy and, increasingly, how we allocate power within it. The Federal Trade Commission (FTC) has played a key role in the U.S. approach to regulation of platforms. Using its relatively old and analog mandate to protect consumers and competition, the agency has adapted its authority over unfair methods of competition and unfair and deceptive practices to today's digital world, where online platforms play a conspicuous role in the daily lives of consumers and the overall economy. Under the FTC's harm-focused, enforcement-based approach to competition enforcement and issues of data collection and use, online platforms—and the innovation that flows from them—have flourished. In fact, some say certain online platforms have flourished too much and gained too much power because of the historically "light touch" regulatory approach in the United States.[1] Our policy conversation has tended to

1. *See, e.g.*, Howard A. Shelanski, Information, *Innovation, and Competition Policy for the Internet*, 161 U. Pa. L. Rev. 1663, 1667 (2013) ("[D]igital platforms raise competitive concerns related to innovation and customer information that may warrant increased antitrust scrutiny of their conduct and merger activity.").

focus on the power of the very large, very successful platforms—sometimes called foundational platforms.[2] These platforms, turbocharged by better technology, improved computing power, and expansive connectivity, are "platforms for platforms" and include, for example, internet service providers, social networks, and operating systems that connect users with app developers. They wield enormous power in the digital economy, thus provoking an important debate about whether our current frameworks for privacy, data use, and competition are sufficient. While remaining mindful of this landscape, it is important to recognize that online platforms come in all shapes and sizes. The multi-sided platform business model is hardly new,[3] and successfully adapting it to the online world is challenging. Failure is common.[4]

If we want policies that both protect consumers and competition and optimize innovation, the FTC must continue to adapt to the changing marketplace. This Essay will begin with some historical background on the FTC; then review the agency's current approach to platforms and some of the benefits and drawbacks of its harm-focused, enforcement-based framework; and finally conclude by examining whether the FTC can keep pace with transformative platforms in the digital economy.

II. HOW THE FTC EMERGED AS A KEY REGULATOR OF ONLINE PLATFORMS

The FTC is, first and foremost, an enforcement agency. Primarily it shapes law and policy by bringing cases against companies that violate the FTC Act or any of the approximately seventy other laws it enforces or administers.[5] But the agency is also charged with shaping policy by studying trends and changes in the marketplace. It does that by issuing reports, holding workshops, and conducting studies to inform its enforcement.[6]

---

2. *See* DAVID S. EVANS & RICHARD SCHMALENSEE, MATCHMAKERS: THE NEW ECONOMICS OF MULTISIDED PLATFORMS 40 fn. 3 (2016).

3. *See id.* at 199–201.

4. *See id.* at 150–156 (noting common struggles of adapting multi-sided platforms to the online world, and identifying signs of failure).

5. *See Enforcement*, FED. TRADE COMM'N (last visited July 17, 2017), https://www.ftc.gov/enforcement.

6. *Policy*, FED. TRADE COMM'N (last visited July 17, 2017), https://www.ftc.gov/policy. *See also* 15 U.S.C. § 46 (2012) (describing the FTC's ability to conduct wide-ranging studies and publish reports that do not have a specific law enforcement purpose, including the power to issue orders requiring companies to answer questions and provide other information to the agency).

Congress established the FTC in 1914.[7] At that time of rapid economic growth and concern about the limited reach of the existing antitrust laws,[8] people worried about the power of enormous, integrated companies that controlled all major networks and commerce and were owned by a very few, very powerful elite.[9] Accordingly, Section 5 of the FTC Act gave the agency broad latitude to address "unfair methods of competition."[10] This mandate was intended to allow the FTC to keep pace with the American marketplace.[11] The prescient founders of the FTC even appear to have addressed issues alive today in the regulation of online platforms, such as the relationship between the allocation of power in the marketplace and access to data. For example, Louis Brandeis noted, "there is one respect in which the great industry has an important advantage. That is in the

7. *About the FTC*, FED. TRADE COMM'N (last visited July 17, 2017), https://www.ftc.gov/about-ftc.

8. In support of a new Commission, Theodore Roosevelt wrote: "it [is] evident that the Anti-Trust Law is not adequate to meet the situation that has grown up because of modern business conditions . . . ." Theodore Roosevelt, *The Trusts*, *the People*, *and the Square Deal*, 99 OUTLOOK 649, 651 (1914), http://www.unz.org/Pub/Outlook-1911nov18-00649a02. America's first antitrust law, the Sherman Act, was not *forward*-looking and, therefore, not designed to preempt anticompetitive practices in their incipiency. Congress passed the Sherman Act in 1890 to safeguard competition and to prevent the consolidation of economic power. But by the second decade of the 20th century there was a growing recognition that the Sherman Act alone was unequal to the task. As Kintner's treatise on antitrust law puts it, "[i]ndifference and failure characterized early United States antitrust policy." 3 EARL. W. KINTNER, ET AL., FED. ANTITRUST LAW § 18.2 (Matthew Bender 2016). A number of the government's challenges to the trusts that dominated the U.S. economy had failed under the Sherman Act. For example, the government challenged the Knight Company's purchase of four other sugar refineries, which gave Knight control of over 98 percent of domestic sugar refining capacity. But the Supreme Court held that Knight's control over refining would have only an "indirect" effect on trade, "however inevitable, and whatever its extent," and was thus outside the purview of the Sherman Act. *Id.*; *United States v. E. C. Knight Co*., 156 U.S. 1, 16 (1895). By 1914, Senator William Thompson (Kansas) found that more than 9,877 previously independent companies had combined to form 628 trusts—with the greatest period of consolidation occurring *after* the enactment of the Sherman Act. *See* 1 JULIAN O. VON KALINOWSKI ET AL., ANTITRUST LAWS AND TRADE REGULATION § 9.03 n. 12 (Matthew Bender 2d ed. 2017); 51 CONG. REC. S14217–18 (1914) (statement of Sen. Thompson).

9. *See* Marc Winerman, *The Origins of the FTC: Concentration*, *Cooperation*, *Control*, *and Competition*, 71 ANTITRUST L.J. 1, 7 (2003) (citing LOUIS BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT (1913)) ("[A] so-called 'money trust' had organized consolidations across multiple industries, and its representation on multiple boards of directors was perceived to create cross-industry interconnections short of merger.").

10. *See* Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2012).

11. *See* Neil W. Averitt, *The Meaning of "Unfair Methods of Competition" in Section 5 of the Federal Trade Commission Act*, 21 B.C. L. REV. 227, 237 (1980).

collection, the getting of knowledge, the collection of data in regard to trade, that knowledge for which great concerns extend their bases of inquiry all over the world."[12] Brandeis argued the FTC could serve to help small businesses gain access to the same information to compete in new markets.[13]

The FTC's original enforcement authority was limited to harm to businesses arising from unfair methods of competition.[14] Although the FTC handled a wide range of complaints—including accusations of predatory pricing, induced breaches of contract, misbranding, boycotts, and theft of trade secrets[15]—it was powerless to protect consumers absent a provable harm to competition. The inadequacy of this authority was highlighted in *FTC v. Raladam*,[16] where the Supreme Court refused to uphold an FTC complaint and injunction against a manufacturer of a harmful substance being marketed as an obesity cure because there was no evidence that the advertising of the product as such was harming any business interests or competition.[17] Congress reacted to this development and in 1938 granted the FTC power to take action against "unfair or deceptive acts or practices" under its Section 5 authority.[18] The Wheeler-Lea Amendments gave the FTC the power to stop harms to consumers without the need to show harm to competitors first, enabling the FTC to begin in earnest its mission of consumer protection.[19] In 1973, Congress solidified this power by granting the Commission authority to seek

12. JEFFREY ROSEN, LOUIS D. BRANDEIS: AMERICAN PROPHET 65 (2016).

13. *See id.*

14. *See* Fed. Trade Comm'n v. Raladam Co., 283 U.S. 643, 649 (1931) ("[T]he trader whose methods are assailed as unfair must have present or potential rivals in trade whose business will be . . . injured. It is that condition of affairs which the Commission is given power to correct . . . and not some other.").

15. *See* FED. TRADE COMM'N, ANN. REP. FOR THE FISCAL YEAR ENDED JUNE 30, 1916, at 5.

16. *See Raladam*, 283 U.S. at 649 ("[T]he unfair methods must be such as injuriously affect or tend thus to affect the business of these *competitors* . . . .") (emphasis added).

17. *See id.* at 652–53; Milton Handler, *The Jurisdiction of the Federal Trade Commission Over False Advertising*, 31 COLUM. L. REV. 527, 528 (1931) (discussing and excerpting from the Second Circuit's decision in the case, which was upheld by the Supreme Court).

18. *See* Wheeler-Lea Act of 1938, ch. 49, § 3, 52 Stat. 111–12 (codified as amended at 15 U.S.C. §45(a)).

19. *See* Lesley Fair, *FTC Milestones: Weighing in on Weight Loss Cases*, FED. TRADE COMM'N (Dec. 4, 2014, 11:25 AM), https://www.ftc.gov/news-events/blogs/competition-matters/2014/12/ftc-milestones-weighing-weight-loss-cases.

preliminary relief and permanent injunctions in federal court under Section 13(b) of the FTC Act.[20]

The FTC has generally been busy with its mandate, protecting consumers from deceptive marketing, abusive debt collection, illegal telemarketing, frauds, scams, and other harmful financial practices. As consumers have moved consumption from a brick-and-mortar world to a digital one, the FTC has followed along. There, naturally, it encountered online platforms.

A. ANTITRUST ENFORCEMENT AND PLATFORM REGULATION

The FTC has a unique dual mission among federal agencies to protect both consumers and competition. As a competition enforcer, the FTC seeks to contribute to the public understanding of platform markets and the unique consumer benefits and competitive risks associated with platforms.[21] The agency has a long history of advocating against overly restrictive regulatory barriers that prevent new entrants.[22] Frequently this

20. *See* Trans-Alaska Pipeline Authorization Act, Pub. L. No. 93-153, tit. IV, § 408(a)(1), 87 Stat. 576, 591 (1973) ("The Congress hereby finds that the investigative and law enforcement responsibilities of the Federal Trade Commission have been restricted and hampered because of inadequate legal authority to enforce subpenas [sic] and to seek preliminary injunctive relief to avoid unfair competitive practices."); § 408(f) (codified as amended at 15 U.S.C. § 53(b)) (granting the Commission injunctive authority). The Wheeler-Lea Act previously added Section 13(a) of the FTC Act in 1938, giving the agency the ability to seek preliminary injunctions in federal court, but only in cases involving the false advertising of food, drugs, devices, or cosmetics. Wheeler-Lea Act of 1938, ch. 49, sec. 4, § 13(a), 52 Stat. 114–15 (codified as amended at 15 U.S.C. § 53(a)).

21. *See*, *e.g.*, FED. TRADE COMM'N, THE "SHARING" ECONOMY: ISSUES FACING PLATFORMS, PARTICIPANTS & REGULATORS 7 (2016), https://www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facing-platforms-participants-regulators-federal-trade-commission-staff/p151200_ftc_staff_report_on_the_sharing_economy.pdf (describing the role of the FTC's "competition advocacy program, which provides advice and input on competition policy issues," including those raised by sharing economy business models).

22. When internet retailers first began making sales to consumers, incumbent brick-and-mortar retailers sought regulatory protection against these new entrants in a number of markets. The FTC advocated against regulatory barriers to online entry in numerous markets from contact lenses to wine shipments. *See*, *e.g.*, FED. TRADE COMM'N, POSSIBLE ANTICOMPETITIVE BARRIERS TO E-COMMERCE: CONTACT LENSES 24 (2004), http://www.ftc.gov/os/2004/03/040329clreportfinal.pdf; Letter from Todd J. Zywicki, Director of the Office of Policy Planning, Fed. Trade Comm'n, et al. to Assemblyman William Magee, Chairman, New York Assembly Agriculture Comm., et al. (Mar. 29, 2004), http://www.ftc.gov/be/v040012.pdf (advocating for legislation to remove barriers to wine e-commerce). More recently, FTC officials have criticized as "bad policy" state laws designed to protect the automobile dealership model from competition from Tesla's direct-to-consumer sales strategy. *See* Andy Gavil, Debbie Feinstein, and Marty Gaynor,

takes the form of advocating on behalf of platforms, like ride-sharing platforms, and urging local regulators to tailor regulations to legitimate safety and consumer protection issues without impeding entry and competition from new services.[23]

The FTC is also experienced in understanding the economic concepts that underlie the operation of platforms and the markets they create. For example, certain digital markets are more susceptible to consolidation of market power because of how a competitor's scale interacts with the value of the goods or services transacted. More specifically, an increase in users on one side of a two-sided platform increases the platform's value to users on the other side—a phenomenon known as network effects. To start and maintain this feedback loop, platform operators frequently offer their service to users on one side of the market for free. Because the price is zero, competition often occurs in the form of innovation and quality improvements in products to entice as many users as possible to join. Users on the "free" side of a platform may thus be harmed by consolidation, since remaining firms would not have to compete as vigorously for customer share—although since the price is zero, a traditional price-based approach to competition analysis would not capture that harm.

Per the discussion of innovation in the FTC's *Horizontal Merger Guidelines*, the agency looks at both sides of a market in the merger

Who Decides How Consumers Should Shop?, FED. TRADE COMM'N (Apr. 24, 2014, 11:00 AM), http://www.ftc.gov/news-events/blogs/competition-matters/2014/04/who-decides-how-consumers-should-shop.

23. In the last few years, the FTC has submitted comments to multiple cities and taxicab authorities urging that regulations be limited to legitimate safety and consumer protection issues, and not impede competition from new ride-hailing platforms (such as those offered by Uber and Lyft). *See* Letter from Andrew I. Gavil, Director of the Office of Policy Planning, Fed. Trade Comm'n, et al. to the Honorable Brendan Reilly, Alderman – 42 Ward, City of Chicago (April 15, 2014), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-honorable-brendan-reilly-concerning-chicago-proposed-ordinance-o2014-1367/140421chicagoridesharing.pdf; Letter from Andrew I. Gavil, Director of the Office of Policy Planning, Fed. Trade Comm'n, et al. to Mr. Jacques P. Lerner, General Counsel, D.C. Taxicab Comm'n (June 7, 2013), http://ftc.gov/os/2013/06/130612dctaxicab.pdf; Letter from Andrew I. Gavil, Director of the Office of Policy Planning, Fed. Trade Comm'n, et al. to the Honorable Debbie Ossiander, Assembly Member, Seat A, Municipality of Anchorage (Apr. 19, 2013), http://www.ftc.gov/os/2013/04/130426anchoragecomment.pdf; Letter from Andrew I. Gavil, Director of the Office of Policy Planning, Fed. Trade Comm'n, et al. to the State of Colorado Public Utilities Comm'n (Mar. 6, 2013), http://ftc.gov/os/2013/03/130703coloradopublicutilities.pdf.

enforcement context.[24] FTC staff did just that in its recent review of the Zillow-Trulia merger, examining whether the merger between the two largest online real estate listing portals would reduce the combined entity's incentives to innovate—that is, the incentive to develop new features attractive to consumers on the free side of the market.[25] If it is going to police anticompetitive combinations involving online platforms effectively, the FTC must remain vigorous in assessing non-price dimensions of competition, such as competition on privacy, quality, and innovation, in merger review.

Given the presence of network effects, platform operators may organically develop monopoly power. Monopoly power in and of itself is not illegal under U.S. antitrust law. Section 2 of the Sherman Act, however, prohibits anticompetitive behavior by a monopolist that blocks competitive entry.[26] Where there is evidence of anticompetitive exclusionary behavior in digital platform markets, competition enforcers should act. Arguably, the FTC has not used its authority in this regard aggressively enough—perhaps due to worry that antitrust enforcement may blunt the incentives of incumbent firms to innovate or out of concern that antitrust cannot keep pace with rapidly evolving technology markets.[27] For example, antitrust litigation can proceed slowly over the course of many years.[28] By the time a court reaches judgment, the thinking goes, the underlying market may be obsolete, supplanted by something newer and better. But this view simply assumes the existence of the very type of disruptive entry that antitrust law exists to protect. To maximize innovation in digital markets, new entrants must have the opportunity to

24. *See* U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, HORIZONTAL MERGER GUIDELINES § 6.4 (2010), https://www.ftc.gov/system/files/documents/public_statements/804291/100819hmg.pdf.

25. *See* Statement of Commissioner Ohlhausen, Commissioner Wright, and Commissioner McSweeny Concerning Zillow, Inc./Trulia, Inc. (Feb. 19, 2015), https://www.ftc.gov/system/files/documents/public_statements/625671/150219zillowmko-jdw-tmstmt.pdf.

26. Sherman Act of 1890 § 2, 15 U.S.C. § 2 (2015)

27. *See*, *e.g.*, Ronald A. Cass, *Antitrust for High-Tech and Low: Regulation*, *Innovation*, *and Risk*, 9 J.L. ECON. & POL'Y 169, 175–78 (2013); Susan Creighton, *2010 Horizontal Merger Guidelines: The View from the Technology Industry*, THE ANTITRUST SOURCE, Oct. 2010, https://www.wsgr.com/PDFSearch/creighton1010.pdf; Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, THE ANTITRUST SOURCE Dec. 2014, http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/dec14_tucker_12_16f.authcheckdam.pdf.

28. *See, e.g.*, *United States v. Microsoft*, 253 F.3d 34, 48 (D.C. Cir. 2001) ("[I]t is noteworthy that a[n antitrust] case of this magnitude and complexity has proceeded from the filing of complaints through trial to appellate decision in a mere three years.").

test their ideas in the market. The threat of enforcement may deter dominant firms from engaging in harmful conduct. Left unchecked, these dominant firms may have an incentive to engage in anticompetitive exclusionary behavior that would slow or prevent new entrants. Thus, while there are challenges associated with antitrust enforcement in rapidly evolving markets, the consequences of the alternative— the FTC simply walking off the field—would be far worse.

B. CONSUMER PROTECTION AND PLATFORM REGULATION

FTC consumer protection cases involving platforms tend to involve the application of longstanding legal principles forged by the FTC's decades of experience with deceptive or unfair advertising and marketing practices. They have also included policing disclosures and controls around in-app purchases by children,[29] deceptive employment opportunity claims made by ride-sharing platforms,[30] revenge-porn,[31] and deceptive use of crowd-funding platforms.[32]

Of course, platforms tend to be information intensive. So much of the FTC's focus has also been on the information privacy and security practices of platforms. In the last decade, the FTC has taken enforcement

29. *See FTC*, *Amazon to Withdraw Appeals*, *Paving Way for Consumer Refunds Related to Children's Unauthorized In-App Charges*, FED. TRADE COMM'N (Apr. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/04/ftc-amazon-withdraw-appeals-paving-way-consumer-refunds-related; *Google to Refund Consumers at Least $19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children's Unauthorized In-App Charges*, FED. TRADE COMM'N (Sept. 4, 2014), https://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it; *Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent*, FED. TRADE COMM'N (Jan. 15, 2014), https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million.

30. *See Uber Agrees to Pay $20 Million to Settle FTC Charges That It Recruited Prospective Drivers with Exaggerated Earnings Claims*, FED. TRADE COMM'N (Jan. 19, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/uber-agrees-pay-20-million-settle-ftc-charges-it-recruited.

31 *Website Operator Banned from the 'Revenge Porn' Business After FTC Charges He Unfairly Posted Nude Photos*, FED. TRADE COMM'N (Jan. 29, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/website-operator-banned-revenge-porn-business-after-ftc-charges; *FTC and Nevada Seek to Halt Revenge Porn Site*, FED. TRADE COMM'N (Jan. 9, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/ftc-nevada-seek-halt-revenge-porn-site.

32. *See Crowdfunding Project Creator Settles FTC Charges of Deception*, FED. TRADE COMM'N (June 11, 2015), https://www.ftc.gov/news-events/press-releases/2015/06/crowdfunding-project-creator-settles-ftc-charges-deception.

action against many major online platforms, including Twitter,[33] Google,[34] Facebook,[35] Snapchat,[36] and Ashley Madison.[37] Some of these cases, like the Twitter case, involved alleged misrepresentations about security practices.[38] Others alleged misrepresentations about privacy practices[39] or, in the case of Snapchat, misleading statements about the ephemerality of images and videos sent through the messaging app.[40]

The agency's recent case involving Ashley Madison—a dating website for individuals who are married or in committed relationships but interested in having affairs with other adults—primarily focused on the site's data security practices, but also included allegations that the website operator made misleading promises to remove users' "digital trail[s]" and induced users into upgrading to paid memberships by use of fake dating profiles.[41] These so-called "engager profiles" were allegedly created by

33. *Twitter Settles Charges That It Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program*, FED. TRADE COMM'N (June 24, 2010), https://www.ftc.gov/news-events/press-releases/2010/06/twitter-settles-charges-it-failed-protect-consumers-personal.

34. *FTC Charges Deceptive Privacy Practices in Googles* [sic] *Rollout of Its Buzz Social Network*, FED. TRADE COMM'N (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

35. *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, FED. TRADE COMM'N (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

36. *Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False*, FED. TRADE COMM'N (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

37. *Operators of AshleyMadison.com Settle FTC*, *State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information*, FED. TRADE COMM'N (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting.

38. Complaint ¶¶ 13–14, In the Matter of Twitter, Inc., Fed. Trade Comm'n Matter No. 0923093 (Mar. 2, 2011) (Docket No. C-4316), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf.

39. *See*, *e.g.*, Complaint ¶¶ 17–18, In the Matter of Facebook, Inc., Fed. Trade Comm'n Matter No. 0923184 (July 27, 2012) (Docket No. C-4365), https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.; Complaint ¶ 6, In the Matter of Google Inc., Fed. Trade Comm'n Matter No. 1023136 (Oct. 13, 2011) (Docket No. C-4336), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf.

40. Complaint ¶¶ 6, 16–17, In the Matter of Snapchat, Inc., Fed. Trade Comm'n Matter No. 1323078 (Dec. 23, 2014) (Docket No. C-4501), https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.

41. Complaint ¶¶ 23–29, 17–22, Fed. Trade Comm'n v. Ruby Corp., No. 1:16-cv-02438 (D.D.C Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf.

staff acting as female users.[42] In reality, about 16 million of the 19 million dating profiles of users in the United States were created by men, yet the company promised users "thousands of women" in the user's city were on the platform.[43]

These cases stem from the evolution of the FTC over the last two decades into the nation's chief federal privacy and information security enforcer. All told, the FTC has brought more than 500 cases protecting the privacy or security of consumer information.[44] The FTC's efforts have focused on holding companies accountable for the promises they make about the information they use and collect, consistently emphasizing the need for firms to offer consumers transparency and choice.[45]

Over time, the FTC has taken the view that consent for collection, sharing, and use of information may be inferred based on consumers' reasonable expectations consistent with the context of a particular transaction.[46] Under this approach, the FTC has supported frameworks requiring opt-in consent for the collection and sharing of sensitive information—including the content of communications; social security numbers; health, financial, and children's information; and precise geolocation data.[47] Importantly, as technology and techniques used to track and profile people online have grown increasingly powerful, the

42. *Id.* at ¶ 18.

43. *Id.* at ¶¶ 12, 17–18.

44. Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Věra Jourová, Comm'r for Justice, Consumers, and Gender Equality, European Commission, at 3 (Feb. 23, 2016), https://www.ftc.gov/public-statements/2016/02/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice.

45. *See*, *e.g.*, FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2016 at 2–5.

46. FED. TRADE COMM'N REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 27, 36–40 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter PRIVACY REPORT] ("Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment.").

47. Comment Before the Federal Communications Commission, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Staff of the Bureau of Consumer Protection of the Fed. Trade Comm'n, WC Dckt. 16-106, FCC 16-39, at 21–22 (May 27, 2016) (https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf); PRIVACY REPORT, *supra* note 46, at 47–48, 58–60 ("Companies should obtain affirmative express consent before . . . collecting sensitive data for certain purposes.").

FTC has updated its understanding regarding what data are personally identifiable and warrant privacy protections.[48] In situations where a company makes material changes to its policies for handling consumer information—particularly how such information is made public—the agency has also required notice and choice.[49]

III. LESSONS LEARNED FROM THE FTC'S ENFORCEMENT ORIENTED APPROACH

There are benefits and drawbacks of relying on the FTC to regulate online platforms. The decades of debate and hundreds of thousands of pages of scholarly opinion on the subject of the relative merits of a regulation, enforcement, or free-market approach to economic policy are beyond the scope of this Essay. Nonetheless, the FTC's fact-based, enforcement-oriented approach arguably lowers the cost and burdens on new entrants and maximizes incentives to innovate.[50] The FTC's focus is economically and technologically informed and primarily harm-based. It is technology neutral and sufficiently flexible to keep pace with a rapidly changing marketplace. Issues of industry capture of a regulator are generally lessened at an enforcement agency with broad authority.

There are drawbacks, of course. The most common complaint is that the FTC does not provide sufficiently clear guidance on how and when it uses its generalized authority.[51] Other critics argue the agency does not

48. Jessica Rich, *Keeping Up with the Online Advertising Industry*, FED. TRADE COMM'N (Apr. 21, 2016, 10:30 AM), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry (discussing the FTC's position that information is "personally identifiable" and deserving of privacy protections "when it can be *reasonably linked* to a particular person, computer, or device. In many cases, persistent identifiers such as device identifiers, MAC addresses, static IP addresses, or cookies meet this test.") (emphasis in original).

49. *See*, *e.g.*, Complaint ¶ 29, In the Matter of Facebook, Inc., Fed. Trade Comm'n Matter No. 0923184 (July 27, 2012) (Docket No. C-4365), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf (challenging material retroactive changes to the company's privacy policy); Decision and Order, Part II, In the Matter of Facebook, Inc., Fed. Trade Comm'n Matter No. 0923184 (July 27, 2012) (Docket No. C-4365), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf (requiring affirmative express consent prior to sharing any nonpublic user information with a third party).

50. *See*, *e.g.*, Shelanski, *supra* note 1, at 1705 (acknowledging the difficulties of "conventional competition enforcement against digital platforms," but arguing for fact-based antitrust enforcement based upon evidence of "effects on innovation incentives").

51. *See*, *e.g.*, Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 249–259 (3d. Cir. 2015) (discussing and dismissing the defendant's argument that the FTC failed to provide fair notice of the specific cybersecurity standards the company was supposed to follow).

confine itself enough to purely economic harms, and it cannot keep pace with an innovative and dynamic marketplace.[52] Those who support more aggressive regulation argue the FTC's modern mandate is optimized to stop practices inflicting concrete harms on consumers and competition, so the agency cannot address broader public interest concerns arising from the power of online platforms in our digital economy.[53]

In fact, there are limitations to relying on a purely enforcement-based approach and downsides to relying on an overly regulatory one. For example, some harms to innovation are hard to detect and equally hard to remedy through *ex post* enforcement. In those situations a hybrid system of clear, appropriately tailored *ex ante* rules coupled with *ex post* enforcement may be justified. The FCC's Open Internet order[54] is arguably justified by the relative concentration of broadband markets, the economics of the virtuous cycle (innovation at the edge spurring demand for broadband), protection of non-economic values like speech, and potential harms that are not easily remedied by antitrust or consumer protection laws.[55]

Moreover, as consumers connect more and more devices in their homes and on their bodies, the array of technology that raises privacy and security concerns grows. Accordingly, the FTC must renew efforts to work with other expert industry regulators. Differences between technologies—and the risks associated with them—may justify some differences in how security and privacy are regulated.[56] For example, the

52. *See*, *e.g.*, Joshua D. Wright, Prof., George Mason Univ. School of Law, Briefing on Nomi, Spokeo, and Privacy Harms at the George Mason University Law & Econ. Center: The FTC and Privacy Regulation: The Missing Role of Economics, at 5–6 (Nov. 12, 2015), http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.

53. *See*, *e.g.*, *Net Neutrality: Is Antitrust Law More Effective Than Regulation in Protecting Consumers and Innovation?: Hearing Before the Subcomm. on Reg. Reform, Commercial, and Antitrust Law of the H. Comm. on the Judiciary*, 113th Cong. 72–75 (2014) (statement of Tim Wu, Professor of Law, Columbia Law School), https://judiciary.house.gov/wp-content/uploads/2016/02/113-111-88377.pdf.

54. FED. COMMC'NS COMM'N, REPORT AND ORDER ON REMAND, DECLARATORY RULING, AND ORDER IN THE MATTER OF PROTECTING AND PROMOTING THE OPEN INTERNET (2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1_Rcd.pdf.

55. *See* Comment Before the Federal Communications Commison, In the Matter of Restoring Internet Freedom, Commissioner Terrell McSweeny, WC Docket No. 17-108 (July 17, 2017) (https://www.ftc.gov/system/files/documents/public_statements/1231533/mcsweeny_-_fcc_comment_7-17-17.pdf).

56. *See*, *e.g.*, Deirdre K. Mulligan & Kenneth A. Bamberger, *Public Values*, *Private Infrastructure and the Internet of Things: The Case of Automobiles*, 9 J.L. & ECON. REG. 7, 27 (2016) (discussing cybersecurity as having characteristics of a public good that

regulations for connected cars, medical devices, and drones may vary from those required for connected toasters and hairbrushes. In these situations the FTC should work with expert industry regulators to craft a policy that is both right for the industry and consistent with the FTC's longstanding framework.[57]

Finally, as new issues arise, the FTC does occasionally need new authorities. Sometimes Congress grants the agency rulemaking authority to address certain practices. For instance, with the rise of internet usage by children, the FTC promulgated the Children's Online Privacy Protection Act Rule (COPPA Rule)[58] in late 1999 pursuant to the Children's Online Privacy Protection Act of 1998.[59] Among other things, the FTC's COPPA Rule requires operators of websites and online services directed at children to obtain verifiable parental consent before collecting children's personal information.[60] In other instances, Congress declares specific practices to be unfair or deceptive under the FTC Act, and grants the agency authority to enforce new laws. Most recently, Congress charged the agency with enforcing the Consumer Review Fairness Act of 2016,[61] which protects

requires consideration of potential risks and which may give rise to a heightened need to improve cybersecurity).

57. For instance, the Federal Trade Commission and its Director of the Bureau of Consumer Protection have filed comments with the National Highway Traffic Safety Administration (NHTSA) regarding vehicle-to-vehicle communications and the Department of Transportation's Federal Automated Vehicles Policy. *See FTC Provides Comment to NHTSA on Privacy and Vehicle-To-Vehicle Communications*, FED. TRADE COMM'N (Oct. 24, 2014), https://www.ftc.gov/news-events/press-releases/2014/10/ftc-provides-comment-nhtsa-privacy-vehicle-vehicle-communications; *FTC's Bureau of Consumer Protection Director Comments on NHTSA's Federal Automated Vehicle Policy*, FED. TRADE COMM'N (Nov. 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftcs-bureau-consumer-protection-director-comments-nhtsas-federal.
Also, in conjunction with NHTSA, the FTC hosted a workshop on privacy and security issues related to connected vehicles in June 2017. *See Connected Cars: Privacy*, *Security Issues Related to Connected*, *Automated Vehicles*, FED. TRADE COMM'N (last visited Nov. 27, 2017), https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.

58. 16 C.F.R. § 312 (2016).

59. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–06 (2012).

60. 16 C.F.R. § 312.3(b) (2016).

61. Consumer Review Fairness Act of 2016, Pub. L. No. 114–258, 130 Stat. 1355. Also, prior to passage of this Act, the Commission had challenged contractual "gag clauses" prohibiting consumer reviews as an unfair practice under Section 5 of the FTC Act. *See*, *e.g.*, *FTC Sues Marketers Who Used "Gag Clauses," Monetary Threats*, *and Lawsuits to Stop Negative Consumer Reviews for Unproven Weight-Loss Products*, FED. TRADE COMM'N (Sept. 28, 2015), https://www.ftc.gov/news-events/press-releases/2015/09/ftc-sues-marketers-who-used-gag-clauses-monetary-threats-lawsuits.

people's ability to share their honest opinions by prohibiting contract terms that ban or restrict honest product reviews; and the Better Online Ticket Sales (BOTS) Act of 2016,[62] which prohibits the circumvention of a security measure or access control system for online purchase of event tickets, *e.g.*, the use of bots that can buy up large numbers of tickets almost instantaneously.[63]

IV. KEEPING PACE WITH PLATFORMS IN THE DIGITAL ECONOMY

As outlined above, there are benefits to the FTC's enforcement-based approach, and also situations in which the FTC must work with expert regulators to craft appropriate solutions. Much of that is possible within the FTC's existing authority, but sometimes the FTC needs grants of additional authority. To keep pace with the rapid expansion of online platforms in the digital economy the FTC must continue to adapt its analog authorities to the digital world.

In the last year especially, the role and power of platforms in our daily lives have been on vivid display—from the potential for manipulation of social media users to the rise of "fake" news. These concerns are feeding a more generalized fear about the economic and politcal power of platforms. Our rapidly expanding connectivity exacerbates some of these concerns, raising questions for policymakers such as:

- How do we optimize for rapid innovation in order to remain a world leader in the development of new technology while mitigating some of the consequences of all this change? Particularly, how do we address digital divides, ensure data sets are high-quality and representative, increase digital readiness, and protect jobs, privacy, and security?
- How do we respond to changing social norms around data sharing?
- How do we make sure consumers, who want to benefit from innovation, still have choice and transparency?
- What additional protections do consumers need?
- Can notice and choice continue to work as the paradigm to protect privacy, especially when choice is increasingly a take-

62. Better Online Ticket Sales Act of 2016, Pub. L. No. 114–274, 130 Stat. 1401.

63. *See* Lesley Fair, *BOTS Act: That's the ticket!*, FED. TRADE COMM'N (Apr. 7, 2017, 12:40 PM), https://www.ftc.gov/news-events/blogs/business-blog/2017/04/bots-act-thats-ticket.

it-or-leave-it proposition where one must accept certain terms to use a particular service?

- As the technology becomes smarter, how and when do we protect human agency?

Not all of these issues fall within the FTC's jurisdiction, but many do. The lessons that the FTC has learned over two decades of protecting consumers and competition online can help inform the kinds of policies needed to address many of these issues. The good news is that the FTC does not need a radically new toolbox. But it does need to continue to use the tools it has—all of them—and continue to evolve along with the marketplace.

A. PROTECTING THE PRIVACY CHOICES OF CONSUMERS

The FTC plays a vital role in protecting consumer access to truthful information about how their personal data are being collected and used, and ensuring that platforms are honoring consumer choices once they are made. In this regard, the role of consumer expectation should continue to be central to FTC enforcement.

Recent cases demonstrate the types of deceptive and unfair information practices the FTC should target. For example, in the FTC's case against InMobi, the FTC alleged that the mobile advertising network used technology to track geolocation even when consumers had denied permission to access their location information, thereby specifically overriding a clearly expressed consumer choice regarding sensitive personal information.[64] In a case against another mobile advertising network, the FTC alleged that Turn, Inc., which participated in a Verizon Wireless program that uniquely identified each Verizon Wireless user through the use of tracking header identifiers appended to their mobile internet traffic, deceived consumers by leading them to believe they could reduce the extent to which the company tracked them on their mobile phones.[65] Finally, television manufacturer VIZIO, Inc. agreed to pay $2.2 million to settle FTC charges that it collected viewing data on 11 million

64. *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission*, FED. TRADE COMM'N (June 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.

65. *Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices*, FED. TRADE COMM'N (Dec. 20, 2106), https://www.ftc.gov/news-events/press-releases/2016/12/digital-advertising-company-settles-ftc-charges-it-deceptively.

smart TVs without consumers' knowledge or consent.[66] The company also agreed to a stipulated order requiring it to disclose prominently and obtain affirmative express consent for its data collection and sharing practices.[67]

Increasingly sophisticated technology that passively gathers detailed information—including sensitive data—raises questions of when consumers ought to have choices over the collection and use of such information. In some situations, the FTC has taken proactive steps to warn consumers about the use of this kind of technology that gathers information without proper notice and consent. For example, the FTC has issued warning letters to app developers using Silverpush software designed to monitor consumers' television use through audio beacons,[68] and urged companies engaged in cross-device tracking to obtain affirmative consent before using cross-device tracking on children or tracking users across their device graphs on sensitive information like health, finances, and geolocation.[69] Similarly, the FTC has recommended that Congress enact legislation allowing consumers to opt out of having sensitive information shared with data brokers for marketing purposes.[70]

B. ESTABLISHING BEST PRACTICES AROUND DATA USE

The FTC recognizes consumer data drives valuable innovation to the benefit of consumers—but may simultaneously expose those same customers to risks.[71] Because of these risks, when it comes to consumer data, there are clear legal obligations that go beyond providing clear notice and choice. There is, of course, the obligation to secure consumer

66. *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent*, FED. TRADE COMM'N (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

67. *Id.*

68. *FTC Issues Warning Letters to App Developers Using 'Silverpush' Code*, FED. TRADE COMM'N (Mar. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

69. FED. TRADE COMM'N, CROSS-DEVICE TRACKING 15–16 (2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

70. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY viii, 50 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

71. *See* PRIVACY REPORT, *supra* note 46, at 7–9; FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES 5–12 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [hereinafter BIG DATA REPORT].

information.[72] Additionally, there may be further obligations associated with the use of consumer data. Specifically, it is now possible for technology to predict things about people that they do not even know themselves.[73] But norms are not well established around when consumers ought to be notified these analytics are being used. For example, the average American consumer may not care very much that a platform can predict that she wants to take a vacation to a sunny beach and show her ads accordingly. But she may deeply care if her employer predicts her potential value based on her interest in beach vacations, or if the price she pays for that vacation is higher because of the kind of computer she used to book the trip.

In some cases, as outlined in the FTC's report on big data, analogous equal opportunity, civil rights, and consumer protection laws already apply in the digital world.[74] For example, the FTC enforces the Fair Credit Reporting Act (FCRA),[75] which applies to consumer reporting agencies (CRAs) that compile and sell reports of consumer information that are used, or expected to be used, to make credit, employment, insurance, or housing decisions about consumers. CRAs have numerous obligations under FCRA. They must implement reasonable procedures to ensure the accuracy of consumer reports,[76] provide consumers with access to their information,[77] and provide the ability to correct errors.[78] Companies that use consumer reports also have obligations—such as providing consumers with adverse action notices if they take an adverse action, like denying or rescinding an offer of employment, based on information in a report.[79] Companies must also provide "risk-based pricing" notices if they deny or charge consumers more for credit based on consumer report information.[80]

72. *See* Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; FED. TRADE COMM'N, START WITH SECURITY, A GUIDE FOR BUSINESSES: LESSONS LEARNED FROM FTC CASES 3 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

73. BIG DATA REPORT, *supra* note 71, at 6–7 (providing examples of big data algorithm applications, such as identifying students for advanced classes and predicting life expectancy and genetic predisposition to disease).

74. BIG DATA REPORT, *supra* note 71, at 17–21.

75. Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*. (2012).

76. 15 U.S.C. § 1681e(b).

77. 15 U.S.C. § 1681g(a).

78. 15 U.S.C. §§ 1681i, 1681g(d).

79. 15 U.S.C. § 1681b(b)(3).

80. 16 C.F.R. § 640.3 (2016).

The FCRA can also apply beyond traditional CRAs—for example, to data brokers.[81] In a case against Spokeo, the FTC argued the company was subject to the FCRA because it marketed detailed consumer profiles—compiled from hundreds of online and offline data sources—as an employment screening tool, including to human resources professionals.[82] In a case against data broker Instant Checkmate, Inc., the FTC alleged the company failed to comply with the FCRA in marketing to its customers consumer reports containing information about prospective tenants or employees.[83] The FTC has also taken action against Time Warner Cable[84] and Sprint[85] following their alleged failure to provide FCRA-mandated risk-based pricing notices after offering less favorable credit terms to customers based on consumer report information.

The FCRA has some gaps, though. For instance, it does not apply if a company is using its own data to make credit determinations.[86] But if a third-party company sells an algorithm or provides analytics services based on its own data to make eligibility determinations for client firms, then the third-party company would likely be acting as a CRA, and both it and its clients would likely be subject to the FCRA.[87] Accordingly, companies should be cautious when using big-data analytics to make FCRA-covered eligibility determinations. Companies also need to consider federal equal opportunity laws, civil rights laws,[88] the Genetic Information Nondiscrimination Act,[89] fair housing law,[90] and, of course,

81. BIG DATA REPORT, *supra* note 71, at ii.

82. *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

83. *Two Data Brokers Settle FTC Charges That They Sold Consumer Data Without Complying With Protections Required Under the Fair Credit Reporting Act*, FED. TRADE COMM'N (Apr. 9, 2014), https://www.ftc.gov/news-events/press-releases/2014/04/two-data-brokers-settle-ftc-charges-they-sold-consumer-data.

84. *Time Warner Cable to Pay $1.9 Million Penalty for Violating the Risk-Based Pricing Rule*, FED. TRADE COMM'N (Dec. 19, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/time-warner-cable-pay-19-million-penalty-violating-risk-based.

85. *Sprint Will Pay $2.95 Million Penalty to Settle FTC Charges It Violated Fair Credit Reporting Act*, FED. TRADE COMM'N (Oct. 21, 2015), https://www.ftc.gov/news-events/press-releases/2015/10/sprint-will-pay-295-million-penalty-settle-ftc-charges-it.

86. 15 U.S.C. § 1681a(d)(2)(A)(i) (exempting "report[s] containing information solely [gained from] transactions or experiences between the consumer and the person making the report").

87. BIG DATA REPORT, *supra* note 71, at 15.

88. *See*, *e.g.*, Civil Rights Act of 1964, Pub. L. No. 88-352, 78 Stat. 241.

89. Pub. L. No. 110-233, 122 Stat. 881 (2008).

Section 5 of the FTC Act, which may apply if data products are sold to third parties that use the products for a discriminatory purpose.[91]

The FTC has already started policing situations in which data products are sold for use in scams or fraudulent conduct. The Commission has challenged the sale of data to customers that a company knows or has reason to know will use the data for fraud. For example, the FTC shut down data broker operation Sequoia One, which allegedly sold the information of financially distressed payday loan applicants to third parties who used that information to withdraw millions of dollars from consumers' accounts without their authorization.[92] In 2006, the FTC took action against data broker Choicepoint, Inc., after the personal financial records of more than 163,000 consumers were compromised—leading to at least 800 cases of identity theft—allegedly due to Choicepoint's failure to screen adequately subscribers to its data products and services, including not implementing reasonable procedures to verify or authenticate the identities and qualifications of prospective subscribers.[93]

Therefore, the FTC and other law enforcers have various legal tools to address some of the risks posed by the amount of information consumers are sharing in the digital economy; however, there are areas where a clear consensus has yet to emerge, especially when it comes to non-economic values like human rights and dignity. Americans love new technology and innovation, but they also have a relatively analog set of expectations about how their data are protected and used. For example, people regard health information as sensitive and expect (after years of signing forms in doctors' offices) it is private. So they are often surprised to learn health information provided to websites or generated on wearables is not subject to the same requirements.[94] Or they may be very surprised to see sensitive

90. *See*, *e.g.*, Fair Housing Act, Pub. L. No. 90-284, tit. viii, 82. Stat. 73, 81 (1968).

91. *See* BIG DATA REPORT, *supra* note 71, at iv, 23, 24.

92. *FTC Puts An End to Data Broker Operation That Helped Scam More Than $7 Million from Consumers' Accounts*, FED. TRADE COMM'N (Nov. 30, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million.

93. *ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties*, *$5 Million for Consumer Redress*, FED. TRADE COMM'N (Jan. 26, 2006), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

94. Latanya Sweeney, Chief Technologist, Fed. Trade Comm'n, Address at the FTC Spring Privacy Series: Consumer Generated and Controlled Health Data (May 7, 2014), https://www.ftc.gov/system/files/documents/videos/spring-privacy-series-consumer-generated-controlled-health-data/ftc_spring_privacy_series_-_consumer_generated_and_controlled_health_data_-_transcript.pdf (discussing health data information flows generally and also stating that students who were surveyed

health information on the public internet, even if they accepted terms that said such data would be made public.[95] Similarly, Americans may regard their television viewing habits as sensitive and not expect their smart televisions to be mining second-by-second viewing information about them without consent.[96] At a more basic level, consumers using a mobile app that allows them to use their Android phones as a flashlight would not have any reason to believe that the app would be tracking their geolocation and sharing that information with advertising networks and other third parties.[97]

Some might say Americans simply do not care about sharing their data in exchange for services. In many cases that may be true. But consumers do continue to expect a choice about who has access to their information and are concerned about loss of control over it. For example, 74% of Americans say it is "very important" to be in control of who can obtain information about them, and 91% believe that they have lost control over how companies collect and use their personal information.[98]

This is not to suggest that companies cannot develop new business models that collect and use consumer data in new or unexpected ways. Of course such innovations can provide great utility or convenience to consumers—and even amaze and delight them. But when data practices depart from established norms and expectations, it is critically important that firms are upfront with consumers in providing a clear and complete explanation of what information they are gathering, how it is being used, and with whom it will be shared. And companies should give consumers a choice about sensitive or unexpected data uses at a relevant time and in

expected that most health data outside the data they provide themselves would be covered by HIPAA).

95. This was the case in the FTC's case against Practice Fusion, an electronic health records company that the Commission alleged failed to disclose that consumer reviews of their health care practitioners, which often included sensitive health information, would be publicly available on the internet. *See Electronic Health Records Company Settles FTC Charges It Deceived Consumers About Privacy of Doctor Reviews*, FED. TRADE COMM'N (June 8, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/electronic-health-records-company-settles-ftc-charges-it-deceived.

96. *See Vizio*, *supra* note 66.

97. *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, FED. TRADE COMM'N (Dec. 5, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.

98. Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

proper context to ensure that decisions are well informed and meaningful.[99]

C. ADAPTING EXISTING FRAMEWORKS & UPDATING THE FTC'S TOOLBOX

Consumer choices about how personal data are used are becoming more meaningful, especially since technology is progressively clustering people into like-minded communities and offering consumers increasingly targeted experiences that not only impact how and with whom they communicate but also what opportunities are available to them. In navigating these increasingly difficult waters, the FTC's enforcement experience and policy frameworks can be a helpful guide. The traditional underpinnings of privacy policy—those long terms-of-service agreements that generally go unread—can also be helpful in establishing the data governance requirements for an organization. For years the FTC and privacy advocates have supported the concept of privacy by design, which means including privacy values all along the product development lifecycle to ensure that products consistently reflect the data practice and values of a firm.[100] More recently, the FTC has incorporated this framework into the concept of *data security* by design, which also suggests a process-based approach that includes building with security in mind, implementing training and testing, and avoiding a siloed approach to information security.[101] It is time for the industry and the FTC to engage in a conversation about expanding these frameworks to incorporate governance—and, as technology becomes smarter and more autonomous, ethics by design. Governance and ethics by design would include the following considerations: (1) privacy; (2) security; (3) safety; (4) transparency; (5) choice; (6) explainability; (7) compliance with existing law; (8) testing; (9) data quality; and (10) mitigation and remediation. Many data collection, usage, and analytics practices are entirely opaque to consumers. Absent more aggressive attention to these issues by the FTC

99. *See* PRIVACY REPORT, *supra* note 46, at 49–50 (calling on companies to "offer clear and concise choice mechanisms that are easy to use and are delivered at a time and in a context that is relevant to the consumer's decision about whether to allow the data collection or use. Precisely how companies in different industries achieve these goals may differ depending on such considerations as the nature or context of the consumer's interaction with a company or the type or sensitivity of the data at issue.").

100. *See generally id.*, at 22–32.

101. *See*, *e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD 28–29 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

there may not be sufficient incentives in the marketplace to develop better technology governance practices.

Ultimately, as the technology operating on our data gets smarter—and the machine learning running algorithms become more autonomous—practicing governance and ethics by design can also be used to safeguard human agency. Such precautions and considerations can address the question of when consumers should get a choice and in what situations automated decision-making requires human oversight. Against this backdrop, the FTC has an important job it must continue to do. While the FTC is doing a good job using its 100-year-old authorities to protect consumers in a digital economy, it needs additional tools. Comprehensive privacy and data security legislation at the federal level that includes civil penalty and rule-making authority for the FTC would be helpful.[102] Outdated sector-specific exemptions from FTC authority—like the common carrier exemption[103] and the limitation on enforcement against non-profit entities[104]—should be eliminated to ensure the agency has sufficient jurisdiction. And finally, the FTC needs additional resources, particularly to expand the agency's use of computer scientists and technologists and to enhance the capabilities of the agency's Office of Technology Research and Investigation.[105]

---

102. *See* PRIVACY REPORT, *supra* note 46, at 11–14.

103. 15 U.S.C. § 45(a)(2) (2012).

104. 15 U.S.C. §§ 45, 46, 53 (empowering the Commission to enforce the FTC Act against "persons, partnerships, or corporations"); 15 U.S.C. § 44 (defining "corporation" as an entity "organized to carry on business *for* its own *profit* or that of its members") (emphasis added). *See*, Cmty. Blood Bank of the Kansas City Area, Inc. v. Fed. Trade Comm'n, 405 F.2d 1011, 1022 (8th Cir. 1969) (holding the Act applies to some nonprofit organizations and not others). *But see*, Cal. Dental Ass'n. v. Fed. Trade Comm'n, 526 U.S. 756, 766–8 (1999) (finding the Act does apply to a non-profit entity that carries on business for the profit of its members).

105. *See* Ashkan Soltani, *Booting Up a New Research Office at the FTC*, FED. TRADE COMM'N (Mar. 23, 2015, 11:00 AM), https://www.ftc.gov/news-events/blogs/techftc/2015/03/booting-new-research-office-ftc; *Office of Technology Research and Investigation*, FED. TRADE COMM'N (last visited July 28, 2017), https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation. The Office of Technology Research and Investigation [OTech] replaced the FTC's Mobile Technology Unit, which previously conducted research on mobile technologies and published reports on topics including mobile apps for kids. *See FTC's Second Kids' App Report Finds Little Progress in Addressing Privacy Concerns Surrounding Mobile Applications for Children*, FED. TRADE COMM'N (Dec. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/12/ftcs-second-kids-app-report-finds-little-progress-addressing.

V. CONCLUSION

The FTC can and should continue to play a key role in the U.S. approach to regulation of platforms. It is vital that in so doing the FTC remains true to its core mandate to protect consumers and competition by enabling the innovation and evolution of digital markets. As another FTC founder President Woodrow Wilson said: "The treasury of America does not lie in the brains of the small body of men now in control of great enterprises . . . . It depends upon the inventions of unknown men, upon the originations of unknown men, upon the ambitions of unknown men."[106] This sentiment is still a good North Star for the evolving FTC—as long as we are willing to acknowledge that even that guiding principle needs an update. The "treasury of America" depends on the inventions, originations, and ambitions of unknown women, too.

106. RONALD J. PESTRITTO, WOODROW WILSON: THE ESSENTIAL POLITICAL WRITINGS 112 (2005).

PLATFORM MARKET POWER

Kenneth A. Bamberger[†] *& Orly Lobel*[††]

ABSTRACT

The rise of the platform economy has been the subject of celebration and critique. Platform companies like Uber, Airbnb, and Postmates have been rightfully celebrated as positively disruptive, introducing much–needed competition in industries that have been otherwise over–mature and stagnant. However, some of the leading new platforms have had such meteoric success that their growing market dominance and technical capacity raise questions about new forms of anticompetitive practices, and negative impacts on consumer and employee welfare.

In this Essay, we develop a framework for considering the market power of platform companies that use digital technology to connect a multisided network of individual users. Specifically, we use the example of Uber as a lens to identify eight questions that are important for assessing platform power. These questions address the way a range of issues play out in the platform context, including more traditional competition concerns around innovation, regulatory arbitrage, barriers to entry, and price setting through platforms' use of the network form to coordinate transactions, the use of digital pricing, and the use of pricing bots. These questions also focus on new concerns about power derived from data collection and use; the use of data to expand into other markets; and the implications of market power for consumer choice about personal privacy.

Together, these questions provide policymakers a framework to consider whether and how questions of market power (and competition more generally) may pose complexity or require analytic adjustments—and how the development of platforms implicates both new opportunities for, and challenges to, consumer and employee welfare in the digital context.

DOI: https://doi.org/10.15779/Z38N00ZT38

† The Rosalinde and Arthur Gilbert Professor of Law, University of California, Berkeley; Faculty Director, Berkeley Center for Law and Technology.

†† Don Weckstein Professor of Law, University of San Diego. Many thanks for helpful comments to participants in the 2017 Platform Law Symposium hosted by the Berkeley Center for Law and Technology, as well as to Steven Davidoff-Solomon, Jordan Barry, Vic Fleisher, and Sam Weinstein; and for stellar research assistance from Ryan Davis, Charles Miller, Haylee Saathoff, and James Teal.

TABLE OF CONTENTS

I. INTRODUCTION

In the past decade, hundreds of new digital companies have changed the ways we consume and share goods, services, and information. The rise of the platform economy has been the subject of celebration and critique. Much of both the praise and the concerns expressed by commentators

surrounds the question of whether new business models such as Uber, Airbnb, and Postmasters are enhancing or decreasing market competition. In many ways platform companies have been rightfully celebrated as positively disruptive, introducing much needed new competition in industries that have been otherwise over–mature and stagnant. And yet, some of the leading new platforms have had such meteoric success that their growing market dominance and technical capabilities raises questions about new forms of anticompetitive practices and negative impacts on consumer and employee welfare.

Notable among these new platform companies is the transportation network company Uber, which already faces several antitrust lawsuits claiming that it engages in anticompetitive practices including price fixing and collusion among its providers. Beyond these lawsuits, there are claims that Uber's pricing scheme is predatory in its intention to drive competition out of the market with below–market prices. Finally—and perhaps most concerning—is the worry that Uber and other platform companies like Airbnb will use their digital power to extract data and information about users in ways that harm consumers and unfairly constrain choices about their privacy. At the same time, Uber itself has launched antitrust lawsuits, claiming that the taxi industries in some localities rely on city regulators to impede competition.

In this Essay, we use the example of Uber as a lens to develop a framework for considering the market power of platform companies that use digital technology to connect a multisided network of individual users. Examining a discrete example provides a concrete perspective for thinking about both positive and negative implications of platforms for innovation and markets, and for consumers and employees.

Looking at Uber also illuminates the important reality that platform companies can be very different from each other in terms of the markets they serve, the type and degree of the power that they exercise within respective markets, and the relative effects of their activities on competition. Newer platform companies such as Uber and Airbnb share characteristics with (relatively) older platforms such as Amazon, eBay, Facebook and Google, in that they use the power and networking capacity of online technology and data analytics to create multisided markets that can quickly scale and achieve market dominance.

But the newer platforms differ from their predecessors in that they are transforming service industries. If Web 1.0 focused on access to information and search, Web 2.0 formed online marketplaces such as Amazon, eBay,

and Craigslist, which focused on the retail industry. The latest platform generation, "Web 3.0," focuses on the service economy and enabling offline interactions by connecting users online. Unlike intangible search engines like Google and Yahoo!, social network platforms like Facebook and LinkedIn, and previous–generation retail platform giants like Amazon and eBay, sharing economy platforms that focus on the service industries have a more physical grounding in local markets. The physical nature of sharing economy platforms has disruptive implications for local incumbents and existing methods of business organization, employment, and pricing.[1] Thus while Uber can provide a lens for examining platform market power generally, it also suggests ways that these differences may have implications for an analysis of pro– or anti–competitive behavior in by Web 3.0 platforms specifically.

II. A FRAMEWORK FOR EVALUATING PLATFORM MARKET POWER

The goals of this Essay are preliminary. In setting forth a framework of questions for considering the different ways that platform market power operates, we do not seek to resolve the questions of whether these market power dynamics, in any particular context, promote or hinder competition or otherwise generate net social harms or benefits. Nor do we advocate particular legal or doctrinal outcomes. Rather, we use the lens of the Uber case to identify eight questions that are important to assessing platform market power. The first two questions ask broadly about market power and consumer harm arising from the specifics of the platform markets: Question One enquires whether the success of the platform under consideration arises from innovation or from undesirable regulatory arbitrage, and Question Two asks when barriers to entry in platform markets stifle competition.

Further, Questions Three, Four, and Five consider implications of platform power on price: specifically, whether a platform's use of the network form to coordinate transactions constitutes price fixing; whether a platform's use of digital pricing is anticompetitive because its use of pricing bots constitutes either illicit tacit collusion or unfair first–order price discrimination; and whether the platform's business model engages in predatory pricing.

1. *See* Vanessa Katz, *Regulating the Sharing Economy*, 30 BERKELEY TECH. L.J. 1067, 1069, 1092 (2015) (describing the disruptive effects of sharing economy platforms on traditional markets).

Finally, Questions Six, Seven, and Eight address issues arising out of the digital nature of platform markets, including when a platform's collection and use of data might raise anticompetitive concerns; when data–related and other elements of the platform market might permit platforms to leverage their power to expand into other markets; and when platform market power might inappropriately restrict consumer choice about personal privacy.

Together, these questions provide policymakers a framework to consider whether and how questions of market power (and competition more generally) may pose complexity or require analytic adjustments. This Essay thus sheds light on how the development of platforms implicates both new opportunities for and challenges to consumer welfare in the digital platform context.

A. QUESTION ONE: IS PLATFORM SUCCESS ATTRIBUTABLE TO MARKET INNOVATION OR UNDESIRABLE REGULATORY ARBITRAGE?

The first question—currently being played out in the courts and political debate—asks whether a platform's operation outside of traditional industry regulations constitutes pro–competitive behavior and substantive economic innovation, or whether its market advantage simply arises from avoiding the costs of consumer and employee protections imposed on its competitors.[2] Online platforms have introduced new business models and innovative technology that alter many of the ways companies provide services and individuals consume and interact.[3] In so doing, they have unleashed a whirlwind of products and services that have the potential to transform most aspects of market consumption, professional engagement, and social interactions.[4] Advances in technology—as well as new business models and changes in lifestyle—combine in the platform in ways that challenge existing, stagnant industries and pushes these industries to change as well.[5] By design, the startup costs to operate a digital platform are low: an app

2. *See, e.g.*, Robert L. Redfearn III, *Sharing Economy Misclassification: Employees and Independent Contractors in Transportation Network Companies*, 31 BERKELEY TECH. L.J. 1023, 1024 (2016) (using examples of Uber and Lyft to examine innovation in context of avoiding traditional regulatory frameworks).

3. *See, e.g.*, Virginia E. Scholtes, *The* Lexmark *Test for False Advertising Standing: When Two Prongs Don't Make a Right*, 30 BERKELEY TECH. L.J. 1023, 1051 (2015) (explaining how "sharing economy businesses" have forced consumer protection law to "stretch to fit changes modern technology has triggered in the economy").

4. Redfearn, *supra* note 2, at 1024.

5. *See* Katz, *supra* note 1, at 1070.

serves as a marketplace.[6] And yet, the very question of operation costs is endogenous to the question of regulation. No doubt some of the savings (though certainly not all or even most) that make platform companies so attractive relate to regulatory arbitrage, choosing business models that avoid regulatory costs, and exploiting the gap between the substance of the deal and its legal treatment.[7]

When it comes to the question of market power and regulation, Uber—the most iconic of the new wave of digital service platforms—is a good place to start. Like Google, Uber has become a verb. Even wedding invitations might suggest "Ubering to the venue" because parking is limited.[8] After years of taxi cab dominance, Uber is becoming for many the preferred way of ride hailing.[9] The idea for Uber was first pitched in 2008.[10] Two years later, in 2010, Uber was tested in New York City and launched in San Francisco.[11] Within a year, Uber expanded to numerous other cities in the United States and had launched internationally.[12] By 2015, Uber provided about 41% of all paid car rides in the United States, taking a significant portion of the market share from taxicab drivers and car rental companies who were down to 20% and 39% of the market share, respectively.[13] By 2017, Uber expanded to 737 cities in eighty–four countries.[14] The only major competitor Uber has in the United States as of

6. *See id.* at 1073.

7. Victor Fleischer, *Regulatory Arbitrage*, 89 TEX. L. REV. 227, 229 (2010).

8. *Travel and Transportation*, THEKNOT (Nov. 2017), https://www.theknot.com/us/zakiya-keys-and-bao-nguyen-nov-2017/details/ ("We are strongly suggesting carpooling and/or Ubering to the venue. It will save you the trouble of driving in circles looking for parking, and you can enjoy your night without being worried about your car.").

9. Sara Swann, *Despite Its Controversies, Uber Was More Popular than Taxis During the 2016 Election*, OPENSECRETS (June 23, 2017), www.opensecrets.org/news/2017/06/uber-more-popular-than-taxis-during-2016/.

10. Julian Chokkattu & Jordan Crook, *A Brief History of Uber*, TECHCRUNCH (Aug. 14, 2014), https://techcrunch.com/gallery/a-brief-history-of-uber/.

11. *Id.*

12. *Id.*

13. Press Release, Certify Inc., Certify Releases its Third Annual SpendSmart™ Report on Current Business Travel Spending Trends (Jan. 21, 2015), www.certify.com/PR-2016-01-20-Certify-Releases-its-Third-Annual-SpendSmart-Report-on-Current-Business-Travel-Spending-Trends.

14. *Uber Cities*, UBER, http://uberestimator.com/cities (last visited Nov. 3, 2017) ("This Uber map shows you Ubers activity around the world, you can click on each of the 84 active countries for a list of supported cities. Check all the fare rates, cars and popular destinations in more than 737 Uber cities.").

late 2017 is Lyft.[15] Lyft has grown quickly throughout 2016 and 2017, stating that in March 2016 it had provided eleven million rides in the United States.[16] Uber, by comparison, provided about fifty million rides in the same month.[17]

The dominance of the taxi industry relied heavily on regulation. Taxis are governed not only through medallion licensing requirements, which are expensive and limited, but also by regulations controlling the rates taxis may charge passengers.[18] Taxi companies thus traditionally enjoyed barriers to entry, which explains in part Uber's success in piercing through these barriers. From this perspective, the strength of Uber's platform is that it operates in a new market segment but competes directly with existing segments. Uber's senior vice president of policy and strategy self–described this dynamic by saying that "[w]e are a technology company, and we're not regulated as a transportation company anywhere in the world."[19] This of course means an inevitable clash between the old guard and the new platforms.

Other commentators seem to share the sentiment that services like Uber are shaking up long–entrenched cartels. That sense is captured in a recent article in Forbes:

> In the States, for far too long for-hire vehicle transport has been heavily regulated to the point of suppressed competition. This lack of competition, driven by taxi companies' donations to local politicians, led to a noticeable decline in taxis' customer service.

15. Eric Newcomer, *Lyft is Gaining on Uber as it It Spends Big on Growth*, S.F. GATE (Apr. 15, 2016, 6:39 PM), http://www.sfgate.com/business/article/Lyft-gaining-on-Uber-as-it-spends-big-on-growth-7251625.php/.

16. *Id.*

17. *Id.*

18. Rafi Mohammed, *Regulation Is Hurting Cabs and Helping Uber*, HARV. BUS. REV. (July 9, 2014), https://hbr.org/2014/07/regulation-is-hurting-cabs-and-helping-uber ("Local governments need to understand that consumers view ride sharing services like Uber as close substitutes to taxis. Regulators are doing its residents an injustice by regulating taxi prices (consumers would benefit from a taxi vs. Uber price war) — and in the process unwittingly fueling Uber's growth and enriching its stockholders.").

19. Faith Hung, *Uber to Go It Alone as It Expands into Southeast Asia*, REUTERS (Nov. 4, 2015, 3:25 AM), http://www.reuters.com/article/us-uber-asia/uber-to-go-it-alone-as-it-expands-into-southeast-asia-idUSKBN12Z15K

> Increased competition fuelled [sic] by ridesharing's growth has even forced taxis to improve their service.[20]

The Washington Post echoed:

> In many cities today, Uber and other ride-sharing businesses are challenging the mutually remunerative alliances between elected officials and taxi cartels. The result is a riot of rentseeking as entrenched interests construe judicial passivity as permission to stifle competition.[21]

Framing Uber's success as the result of overcoming anticompetitive regulation suggests that Uber provides a model capable of creating significant social benefits. Permitting, licensing, and regulatory price controls have long served as barriers to new entry to all types of vocations.[22] Compared to only a few decades ago, the number of occupations that require a license is stunningly high: nearly one–third of jobs.[23] In July 2015, the White House issued a report warning that while some licensing requirements were designed to provide safety and professionalism, "the current licensing regime in the United States also creates substantial costs, and often the requirements for obtaining a license are not in sync with the skills needed for the job."[24] In one amicus brief, a group of antitrust scholars further described contemporary licensing as having been "abused by incumbent market participants to exclude rivals, often in unreasonable

20. Jared Meyer, *Uber Is Not (and Will Never Be) a Monopoly*, FORBES (Feb. 15, 2016, 7:45 AM), https://www.forbes.com/sites/jaredmeyer/2016/02/15/uber-guardian-not-monopoly-ridesharing/.

21. George F. Will, *A Strike Against Rent-Seeking*, WASH. POST (Dec. 31, 2014) www.washingtonpost.com/opinions/george-will-a-strike-against-rent-seeking/2014/12/31/ba5a1686-9109-11e4-ba53-a477d66580ed_story.html.

22. U.S. DEP'T OF THE TREASURY ET AL., OCCUPATIONAL LICENSING: A FRAMEWORK FOR POLICYMAKERS 7 (2015), https://obamawhitehouse.archives.gov/sites/default/files/docs/licensing_report_final_nonembargo.pdf.

23. Brad Hershbein, David Boddy & Melissa S. Kearney, *Nearly 30 Percent of Workers in the U.S. Need a License to Perform Their Job: It Is Time to Examine Occupational Licensing Practices*, BROOKINGS INSTITUTION (Jan. 27, 2015), https://www.brookings.edu/blog/up-front/2015/01/27/nearly-30-percent-of-workers-in-the-u-s-need-a-license-to-perform-their-job-it-is-time-to-examine-occupational-licensing-practices/.

24. U.S. DEP'T OF THE TREASURY ET AL., *supra* note 22, at 3.

ways, and to raise prices. This disturbing trend already costs consumers billions of dollars every year and impedes job growth . . . ."[25]

Critics of Uber, on the other hand, have charged that the platform's model "threatens local democracy"[26] by enabling Uber to benefit at the expense of both consumers and drivers through subversion of important regulatory requirements. With respect to consumers, these regulatory requirements deal with auto safety, driver qualifications, and insurance thresholds, while drivers are protected by regulations governing working standards and compensation levels.[27] In this vein, the taxi industry has claimed that Uber is gaining an unfair advantage by evading the regulatory requirements that have long been imposed on taxis, and class actions have been filed alleging that the company undermined other important legal rights, such as lawsuits by drivers who claim that Uber has misclassified them as independent contractors when they are in fact Uber employees.[28] In a suit filed against Uber, the Philadelphia Taxi Association claimed that Uber, through its reliance on independent drivers and their vehicles, sidestepped the strict city regulations that the taxi associations are required to follow.[29] The plaintiffs claimed that Uber thereby created an unfair marketplace, causing taxi services to lose substantial amounts of business since 2014,[30] and accordingly alleged violations of Section 2 of the Sherman Act.[31] The federal district court dismissed the suit on the grounds that the plaintiffs failed to establish antitrust injury, which requires an allegation of injury to competition.[32] While taxi companies—Uber's competitors—"have

25. Brief of Antitrust Scholars as Amici Curiae in Support of Respondent at 2, N.C. State Bd. of Dental Exam'rs v. FTC, 135 S. Ct. 1101 (2014) (No. 13-534), 2014 WL 3908427.

26. Nathan Newman, *Uber: When Big Data Threatens Local Democracy*, DATA JUST. BLOG (July 17, 2015, 10:55 AM), http://www.datajustice.org/blog/uber-when-big-data-threatens-local-democracy.

27. *See* Brishen Rogers, *The Social Costs of Uber*, 82 U. CHI. L. REV. DIALOGUE 85 (2015) (describing six dimensions of criticism against Uber).

28. Second Amended Class Action Complaint and Jury Demand, O'Connor v. Uber Techs., Inc., 201 F. Supp. 3d 1110, 1113 (N.D. Cal. 2016) (No. CV 13-3826-EMC), 2014 WL 7912596.

29. Phila. Taxi Ass'n, Inc. v. Uber Techs., Inc., 218 F. Supp. 3d 389, 391 (E.D. Pa. 2016).

30. *Id.* at 392.

31. *Id.* at 390.

32. *Id.* at 392.

undoubtedly suffered injury since Uber began operating in Philadelphia," the court concluded, "competition has not."[33]

The antitrust lawsuits against Uber extend beyond the United States. The South African Meter Taxi Association and eight regional taxi companies filed suit against Uber in South Africa in May of 2016.[34] These allegations, much like those in the United States, assert that Uber's practices are contrary to the South African Competition Commission's requirements, as Uber floods the market with below–cost drivers but does not comply with regulations.[35]

Some cities have responded by imposing new regulations targeting the market that the digital company is replacing or the new digital company itself. In countries throughout Europe, for example, Uber is now banned or subject to serious restrictions.[36] Chicago, Austin, and several other cities have taken the approach of imposing new restrictions on Uber itself.[37] Chicago proposed imposing fingerprinting and background checks on Uber drivers in the hopes of regulating and making Uber safer and holding it to the same standards imposed on taxicab companies.[38] Similarly, in February 2015, the city of Orlando passed an ordinance requiring ridesharing companies to charge the same rate as taxis: $2.40 per mile.[39] In contrast,

33. *Id.* at 393. A similar lawsuit brought in Maryland alleged that Uber participated in anti-competitive price fixing and predatory pricing, in violation of Maryland Antitrust Act. *See* Yellow Cab Co. et al. v. Uber Techs., Inc. et al, No. RDB–14–2764, 2015 WL 4987653 (D. Md. Aug. 19, 2015) (remanding to state court).

34. *South African Taxis Lose Bid to Declare Uber Anti-Competitive*, MYBROADBAND (Oct. 20, 2016), http://mybroadband.co.za/news/motoring/183688-south-african-taxis-lose-bid-to-declare-uber-anti-competitive.html.

35. *Id.*

36. Damien Geradin, *Should Uber be Allowed to Compete in Europe? And If So How?*, COMPETITION POL'Y INT'L (June 2015), https://www.competitionpolicyinternational.com/assets/Europe-Column-New-Format.pdf (noting that Uber is strictly regulated in Belgium, France, Germany, Italy, and Spain).

37. John Byrne, *Ride-Share Companies Threaten to Leave Chicago if Tougher Regulations Pass*, CHI. TRIB. (May 26, 2016, 7:26 AM), www.chicagotribune.com/news/local/politics/ct-emanuel-rideshare-debt-collection-met-20160525-story.html; *Uber Regulation: US Cities That Have Successfully Stood Up to Uber*, WHO'S DRIVING YOU? (July 19, 2015), http://www.whosdrivingyou.org/blog/us-cities-stood-up-regulate-uber; Madlin Mekelburg, *Across Texas, Uber Puts Cities in Tough Spot*, TEX. TRIB. (Feb. 3, 2016, 6:00 AM), https://www.texastribune.org/2016/02/03/ride-share-giant-uber-puts-texas-cities-tough-spot/.

38. Byrne, *supra* note 37.

39. Stephen Hudak, *Uber Vows to Pay Drivers' Fines as Orlando Regulations Kick In*, ORLANDO SENTINEL (Feb. 2, 2015, 6:36 PM), www.orlandosentinel.com/news/

some cities chose to enhance competition by deregulating taxi companies instead.[40]

In response to heightened regulation, Uber and other ridesharing providers have pushed back in a variety of ways. In cities where regulation seemed too severe, both Uber and Lyft have simply chosen to leave rather than to fight or comply.[41] For example, in 2016 Uber left Austin and Lyft left Houston after new restrictions regarding background checks for drivers were imposed in each city.[42] Uber has also sought to use antitrust litigation to resist regulation by local agencies, arguing that local rules are decreasing fair competition. In Saint Louis, Uber fought with the St. Louis Metropolitan Taxicab Commission (MTC) which eventually voted in 2015 to allow Uber to operate, but only after drivers were fingerprinted, had a background check, and submitted to other potential regulations.[43] Unsatisfied with those regulations, Uber subsequently filed suit against the MTC, its commissioners, and various St. Louis taxi companies, asserting that the defendants had stifled competition over the ridesharing industry. [44] While the federal judge presiding over the case subsequently dismissed the suit, it was refiled in state court.[45] In Seattle, a city ordinance which sets a framework for collective bargaining and rate setting for drivers in the transportation service industry, including both taxis and Uber, has also been challenged on antitrust grounds.[46]

---

breaking-news/os-uber-orlando-fight-20150202-story.html (noting that Uber has said that it will pay fines of drivers in Orlando).

40. Caitlin Clark, *Bryan City Council OKs First Reading of Uber Regulations*, EAGLE (Mar. 24, 2016), http://www.theeagle.com/news/local/bryan-city-council-oks-first-reading-of-uber-regulations/article_78af4e94-12cb-5f0a-8916-d4a929858c96.html.

41. *See id*.

42. *Id.*

43. Sarah Fenske, *Uber Launches in St. Louis Today, Defying — and Suing — Taxi Commission*, RIVERFRONT TIMES (Sept. 18, 2015, 10:00 AM), www.riverfronttimes.com/newsblog/2015/09/18/uber-launches-in-st-louis-today-defying-and-suing-taxi-commission.

44. Wallen v. St. Louis Metro. Taxicab Comm'n, No. 4:15-cv-1432, 2016 WL 5846825 (E.D. Mo. Oct. 6, 2016); THOMAS A. DICKERSON, TRAVEL LAW § 2.11 (2017).

45. *See* Kevin Killeen, *Federal Judge Sends Uber Lawsuit to State Court*, CBS ST. LOUIS (Aug. 8, 2016, 4:16 PM), http://stlouis.cbslocal.com/2016/08/08/federal-judge-sends-uber-lawsuit-to-state-court/.

46. Chamber of Commerce v. City of Seattle, No. C16-0322RSL, 2016 WL 4595981 (W.D. Wash. Aug. 9, 2016) (dismissing suit for lack of standing); *see also* Kate Andrias, *The New Labor Law*, 126 YALE L.J. 2, 92 n.485 (2016) ("Assuming the drivers are independent contractors who do not qualify for the labor exemption, a likely issue will be

Understanding the net impact of digital platforms, then, requires careful inquiry into both gains generated as platforms disrupt barriers to entry into mature industries, and concomitant threats to regulatory protections at all levels of government—especially because of the ways that Web 3.0 platforms interact with local markets. This means that antitrust law alone, and its traditional categories of analysis, has so far proven an awkward home for considering questions of regulatory balance in a comprehensive way. Both price setting and the creation of other mandates regarding consumer and labor protection "often turn[] on political decisions about levels of service and the rate of return to capital needed to provide those services."[47] This reality suggests a theme throughout each of the questions set forth for considering the challenges raised by platform market power: answers will likely require a range of regulatory analyses and, importantly, better integration between traditional antitrust law approaches and other regulatory fields.

B. QUESTION TWO: DO BARRIERS TO ENTRY IN THE PLATFORM MARKET STIFLE COMPETITION?

The fundamental task of defining market power, and even more basically, identifying the relevant market of a platform, presents new challenges to regulators. The Sherman Act was originally drafted with the idea of preventing steel and large manufacturing monopolies. The same law that was drafted to assess car manufacturing competition might not be well–situated to prevent car sharing applications from forming monopolies. While the Sherman Act makes it illegal to "monopolize, or attempt to monopolize . . . any part of the trade or commerce," it does not define monopoly power.[48] In determining whether a competitor possesses monopoly power in a relevant market, courts typically begin by looking at the firm's market share.[49] Although the courts have not set a precise market

whether the ordinance qualifies for *Parker* immunity, which allows states to enact anticompetitive regulation when acting in their sovereign capacities.").

47. Dennis W. Carlton & Randal C. Picker, *Antitrust and Regulation*, *in* ECONOMIC REGULATION AND ITS REFORM 25 (Nancy L. Rose ed., 2014).

48. 15 U.S.C. § 2 (2012).

49. *See, e.g.*, U.S. Anchor Mfg., Inc. v. Rule Indus., Inc., 7 F.3d 986, 999 (11th Cir. 1993) ("The principal measure of actual monopoly power is market share . . . ."); Movie 1 & 2 v. United Artists Commc'ns, Inc., 909 F.2d 1245, 1254 (9th Cir. 1990) ("[A]lthough market share does not alone determine monopoly power, market share is perhaps the most important factor to consider in determining the presence or absence of monopoly power");

share percentile for inferring monopoly power, they have so far demanded a dominant market share.[50] Discussions of the requisite market share for monopoly power commonly begin with Judge Hand's statement in *United States v. Aluminum Co. of America* that a market share of ninety percent "is enough to constitute a monopoly; it is doubtful whether sixty or sixty-four percent would be enough; and certainly thirty-three per cent is not."[51] The Supreme Court soon endorsed Judge Hand's approach in *American Tobacco Co. v. United States*.[52]

If dominant market share alone were enough, then most courts would likely consider Uber to be a monopoly either today or in the very near future, given Uber's projected growth.[53] Uber's ability to scale rapidly cannot be overstated. A graphic of Uber's growth within the business community in a matter of just thirty months illustrates its growing popularity in domestic markets.[54] Figure 1 reflects the growth in corporate use alone—general adoption by the ride hailing public is even more impressive: Uber has recently reported to a selective group of shareholders that it owns 83–87% of the U.S. market share.[55]

Weiss v. York Hosp., 745 F.2d 786, 827 (3d Cir. 1984) ("A primary criterion used to assess the existence of monopoly power is the defendant's market share.").

50. *See* JEFF MILES, PRINCIPLES OF ANTITRUST LAW 13 (2016), https://www.americanbar.org/content/dam/aba/administrative/healthlaw/01_antitrust_primer_01.authcheckdam.pdf ("No magic market share, by itself, proves market power, because other factors affect the degree of a firm's market power. Many courts, however, suggest that 30% is a minimum threshold requirement.").

51. United States v. Aluminum Co. of Am., 148 F.2d 416, 424 (2d Cir. 1945).

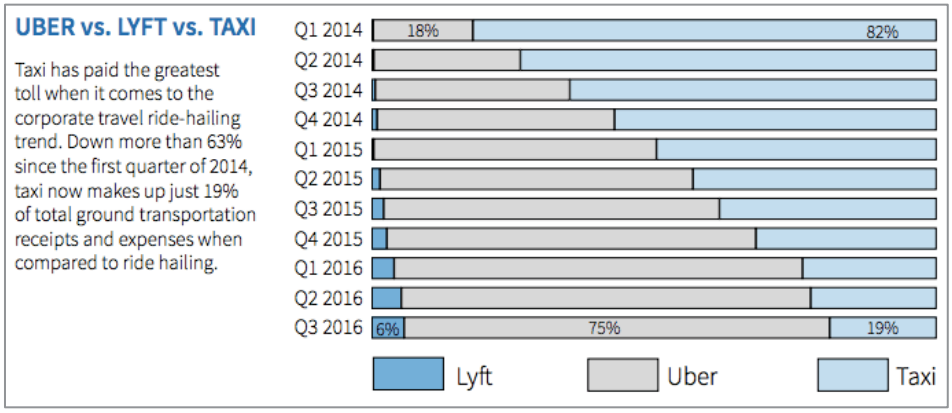
52. *See* Am. Tobacco Co. v. United States, 328 U.S. 781, 813 (1946).

53. *See id.*

54. Ken Yeung, *Uber and Lyft Made Up 52% of Business Travel Transportation Expenses in Q3*, VENTUREBEAT (Oct. 20, 2016, 12:00 AM), http://venturebeat.com/2016/10/20/uber-and-lyft-made-up-52-of-business-travel-transportation-expenses-in-q3.

55. Avery Hartmans, *Uber Says It Has Over 80% of the Ride-Hailing Market in the U.S.*, BUS. INSIDER (Aug. 25, 2016, 9:43 AM), http://www.businessinsider.com/uber-majority-ride-hailing-market-share-lyft-us-2016-8/.

Figure 1: Uber's Relative Share of the Corporate Travel Market, 2014–2016



In this respect, Uber's performance mirrors the success of a range of online platforms. Citing Amazon's share of the print and electronic book markets, Alibaba's share of the e–commerce market, Facebook's domination of social networks, and Google's share of online search, one commentator has noted that in the online platform context, "capturing a significant, even dominant share of the world market more or less straight out of the box is clearly possible . . . . Something about the internet clearly favours such mushrooming quasi-monopolies."[56] Others have argued that platforms are inherently prone to a "winner–takes–all" scenario, whereby "only one or two platforms will dominate an industry as the market matures" because of network effects, since "platforms' margins increase as their networks grow."[57]

Yet recent federal circuit courts have held that, under antitrust analysis, dominant market share alone is not sufficient to establish monopoly power. Instead, "a firm cannot possess monopoly power in a market unless that market is also protected by significant barriers to entry."[58] Accordingly,

56. *Everybody Wants to Rule the World*, ECONOMIST (Nov. 27, 2014), http://www.economist.com/news/briefing/21635077-online-businesses-can-grow-very-large-very-fastit-what-makes-them-exciting-does-it-also-make/.

57. ALEX MOAZED & NICHOLAS L. JOHNSON, MODERN MONOPOLIES: WHAT IT TAKES TO DOMINATE THE 21ST CENTURY ECONOMY 95 (2016).

58. United States v. Microsoft Corp., 253 F.3d 34, 82 (D.C. Cir. 2001) (en banc) (per curiam); *see also* Harrison Aire, Inc. v. Aerostar Int'l, Inc., 423 F.3d 374, 381 (3d Cir. 2005) ("In a typical section 2 case, monopoly power is 'inferred from a firm's possession of a dominant share of a relevant market that is protected by entry barriers.'" (quoting *Microsoft*, 253 F.3d at 51)).

courts have adopted the lens of entry potential, because even when no current rival exists, an attempt to increase price above the competitive level may lead to an influx of competitors sufficient to make that price increase unprofitable.[59] The question of whether platform market power stifles competition, therefore, requires an inquiry into the extent to which the characteristics of such markets create barriers to entry.

1. First–Mover Advantages and Switching Costs

Traditional inquiries into barriers that may prevent the emergence of new competitors focus on the relative disadvantage of being a later entrant into a market, and the extent to which the attributes of that market make later entry prohibitive.[60] Early entry into a field may give an entity substantial competitive advantage through technology leadership, control of

59. *See, e.g.*, PHILLIP E. AREEDA & HERBERT HOVENKAMP, FUNDAMENTALS OF ANTITRUST LAW § 5.01 at 5–7 (4th ed. 2011) ("In spite of its literal imprecision, the standard formulation is essentially correct in asking whether the defendant can price monopolistically without prompt erosion from rivals' entry or expansion.").

60. While the importance of a "first mover" advantage is heatedly debated among economists, Fernando Suarez & Gianvito Lanzolla, *The Half-Truth of First-Mover Advantage*, HARV. BUS. REV. (Apr. 2005), https://hbr.org/2005/04/the-half-truth-of-first-mover-advantage/, as has the importance of being literally the "first," entrant into a platform market, DAVID S. EVANS & RICHARD SCHMALENSEE, MATCHMAKERS: THE NEW ECONOMICS OF MULTISIDED PLATFORMS 27–28 (calling the first–mover advantage and winner–takes–all theories "shaky at best" in the network context, and citing numerous instances in which the first mover did not succeed), the broader question is whether later entrants are at a critical disadvantage in reaching the critical mass necessary to success because of the characteristics of the platform market, *id*. at 69 ("Multisided platforms must secure critical mass, or else"). *See also* Pamela Samuelson, *Functionality and Expression in Computer Programs: Refining the Tests for Software Copyright Infringement*, 31 BERKELEY TECH. L.J. 1215, 1292 (2017) ("A recent empirical study demonstrates that software entrepreneurs consider first mover advantages the most important way to attain advantage."); Misa K. Eiritz, *Should Intellectual Property Owners Just Do It? An Examination into the Effects of Nike's Covenant Not to Sue*, 29 BERKELEY TECH. L.J. 837, 857–58 (2014); Oren Bracha & Talha Syed, *Beyond Efficiency: Consequence-Sensitive Theories of Copyright*, 29 BERKELEY TECH. L.J. 229, 238 n.25 (2014) ("[F]irst-mover advantages or contractual arrangements may guarantee sufficient incentives to create even in the absence of copyright."); Wei Wang, *Non-Practicing Complainants at the ITC: Domestic Industry or Not?*, 27 BERKELEY TECH. L.J. 409, 427 (2012); J. Jonas Anderson, *Secret Inventions*, 26 BERKELEY TECH. L.J.. 917, 967 (2011); Jonathan M. Barnett, *The Illusion of the Commons*, 25 BERKELEY TECH. L.J. 1751, 1763–64 (2010); Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1133, 1152 & n.85 (2009).

resources, and "lock–in" resulting from switching costs.[61] Such consumer lock–in effects hamper market entry by competitors seeking to attract existing customers—especially in markets characterized by network effects, discussed below in Section II.B.[62]

In certain respects, barriers to entry for Web 3.0 competitors are low. On the technological side, a basic platform app may be relatively easy to mimic,[63] and the low startup costs for an internet–based company with little overhead is likely to encourage competition.[64] Moreover, unlike, for example, Amazon—which has acquired vast warehouses which may make it difficult for new competitors to enter the online retail market on a similar scale[65]—similar investments in physical space have not characterized newer platforms.[66] In practice, numerous apps pop up daily in the hopes of competing with companies like Uber, suggesting that the technological advantage and resource control may not significantly impede market entry.

The question of switching costs is more complicated. Consumers can be locked–in to initial brand choices by the direct costs of switching, the time required to learn and ramp up new systems,[67] brand loyalty enhanced by a reluctance to switch away from a trusted network,[68] and even "buyers' choice under uncertainty"—the rational decision to stick with a known

61. Marvin B. Lieberman & David B. Montgomery, *First-Mover Advantages*, 9 STRATEGIC MGMT. J. 41, 41 (1988).

62. Joseph Farrell & Paul Klemperer, *Coordination and Lock-In: Competition with Switching Costs and Network Effects*, *in* 3 HANDBOOK OF INDUSTRIAL ORGANIZATION 1970, 1974 (Mark Armstrong & Robert H. Porter eds., 2007).

63. *See* MOAZED & JOHNSON, *supra* note 57, at 78 (discussing low technical barriers to entry).

64. *See* Deborah R. Ettington & Hal P. Kirkwood, Jr., *First-Mover Advantage*, REFERENCE FOR BUS., http://www.referenceforbusiness.com/management/Ex-Gov/First-Mover-Advantage.html (last visited Mar 16, 2017); Richard J. Gilbert & David M. G. Newbery, *Preemptive Patenting and the Persistence of Monopoly*, 72 AM. ECON. REV. 514, 517 (1982).

65. Rani Molla, *Amazon Takes Up a Lot of Space*, BLOOMBERG (Feb. 4, 2016, 6:45 AM), https://www.bloomberg.com/gadfly/articles/2016-02-04/amazon-takes-up-space-as-a-delivery-giant/.

66. *See generally What Is Web 3.0? A Brief Introduction and It's Benefits*, 1STWEBDESIGNER (Sept. 30, 2016), https://1stwebdesigner.com/what-is-web-3-0/ (describing data and intelligent systems as the focus of Web 3.0).

67. *See* Aaron S. Edlin & Robert G. Harris, *The Role of Switching Costs in Antitrust Analysis: A Comparison of Microsoft and Google*, 15 YALE J.L. & TECH. 169, 176 (2013).

68. Lieberman & Montgomery, *supra* note 61, at 46.

brand that performs satisfactorily.[69] Yet while these lock–in issues were found salient in the technology context in the 1998 Microsoft case,[70] similar phenomena have not been determinative in cases involving online platform context. For example, in 2013, the Federal Trade Commission (FTC) decided not to bring suit against Google Search after Google agreed to change its business practices to resolve competition concerns.[71] The major concern involved reports that Google Search was biased in favor of its own information and search results.[72] The FTC's concerns were primarily resolved by the lack of user lock–in and the low costs of switching to use a different search engine, because most search engines are relatively comparable.[73]

Several emergent characteristics of various platform business, however, suggest that this calculus may function differently as platforms evolve, and will require a context–specific assessment by regulators. Factors that may "lock" users into an incumbent platform include the extent to which a market precludes "multihoming"—the ability for an individual to use multiple platforms to access similar services (i.e. to use both Uber and Lyft equally effectively), technical and contractual barriers to the portability of content developed on one platform to that of a competitor, the collection of data about things like past user behavior that a platform might use to refine services (discussed later in Section II.F), and the system of rating and reviews often integral to the design and value of the Web 3.0 platform model, which creates a system of "strangers trust."[74] The review system means that customers will be more inclined to stay with the service since they have built rapport, and may even receive better service because of their prior dealings.

2. Network Effects

The barriers to entry posed by switching costs are particularly powerful in contexts with strong network effects. Metcalfe's Law proposes that the value of a network is proportional to the square of the number of connected

69. Richard L. Schmalensee, *Product Differentiation Advantages of Pioneering Brands*, 72 AM. ECON. REV. 349, 350 (1982).
70. Elin & Harris, *supra* note 67, at 171.
71. *Id.*
72. *Id.* at 172.
73. *Id.* at 172–73.
74. Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 146 (2016).

users of the system.[75] Discussions of network effects have traditionally focused on "direct" effects, by which increases in usage directly increase the value of the network. A classic example is the fax technology: a single fax machine is useless, but the value of every fax machine increases with the total number of fax machines in the network, because the total number of people with whom each user may send and receive documents increases.[76] Network effects raise potential antitrust issues as entities with larger networks can entrench their dominance and thereby decrease competition.[77]

By contrast, *indirect* network effects traditionally occur when product usage "spawns the production of increasingly valuable complementary goods, and this results in an increase in the value of the original product."[78] In the context of two–sided markets, indirect network effects appear as "cross–side" effects, whereby "the value delivered to each user in one user group (say, consumers) increases as the number of users in another interdependent group (producers) grows."[79] And until a new entrant can amass a critical mass of users on both sides of a new network, it cannot grow and develop into a thriving platform—even if it employs a similarly good, or even better, technology.[80]

In such a fashion, network effects can compound the potential for switching costs to create harmful consumer lock–in. Network effects and

75. CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1999).

76. Rahul Tongia & Ernest J. Wilson III, *The Flip Side of Metcalfe's Law: Multiple and Growing Costs of Network Exclusion*, 5 INT'L J. COMM. 665, 669 (2011).

77. Ronald A. Cass, *Antitrust for High-Tech and Low: Regulation, Innovation, and Risk*, 9 J.L. ECON. & POL'Y 169, 175–76 (2013).

78. Eric Jorgenson, *The Power of Network Effects: Why They Make Such Valuable Companies, and How to Harness Them*, MEDIUM (June 21, 2015), https://medium.com/evergreen-business-weekly/the-power-of-network-effects-why-they-make-such-valuable-companies-and-how-to-harness-them-5d3fbc3659f8. For example, an indirect network effect occurs with the app stores for smartphones: as a smartphone increases in popularity, an increasing number of software engineers will design applications for its specific platform, thus indirectly increasing the value of the smartphone. *See* Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH. L.J. (forthcoming 2017).

79. MOAZED & JOHNSON, *supra* note 57, at 168.

80. *See, e.g.*, Steve Denning, *Five Reasons Why Google+ Died*, FORBES (Apr. 17, 2015, 11:58 AM), https://www.forbes.com/sites/stevedenning/2015/04/17/five-reasons-why-google-died/ (describing how the innovative Google+ network "died" because it could not generate a critical mass of users sufficient to challenge Facebook).

switching costs reinforce each other to create lock–in because consumers must collectively coordinate a costly switch to benefit from a competitor's network.[81] This can lead to substantial collective inertia that gives a dominant firm the opportunity to increase prices, results consumer deadweight loss, and potentially decreases innovation and consumer choice.[82]

Platforms like Uber and Airbnb are two–sided markets coordinated by a digital provider: networks where the customers and providers interact between an intermediary platform. Thus, they rely on network effects which involve two distinct groups that ultimately benefit each other.[83] Scale is critical to the peer–to–peer platform model: for the most part, the greater the number of users in each of the markets, the more valuable the service becomes to the community.[84] Because these platforms utilize individual service providers to bring their product directly to the market, it is easy for the platforms to offer their product on a large scale with decreasing costs as their operations spread. Uber is incentivized to offer their services to any area that wants them because as they increase the number of riders, they can diffuse their fixed costs of developing and maintaining software, and in turn can charge a lower price than anybody else in the market.[85] Moreover, because indirect network effects are particularly powerful when they are localized geographically,[86] Uber can achieve a dominant market position in any of the metropolitan areas in which it operates independent of its market share elsewhere.

---

81. Switching costs discourage large scale entry by a competitor because the pre-existing network of consumers have switching costs. Network effects discourage small scale entry because a network must achieve critical mass to offer value to users. *See* Farrell & Klemperer, *supra* note 62, at 2045.

82. *See id.*; Paul Klemperer, *Competition When Consumers Have Switching Costs: An Overview with Applications to Industrial Organization, Macroeconomics, International Trade*, 62 REV. ECON. STUD. 515, 536 (1995).

83. Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1 J. EUR. ECON. ASS'N. 990, 990 (2003); Jorgenson, *supra* note 78.

84. Jorgenson, *supra* note 78.

85. Eric Posner, *Why Uber Will—and Should—Be Regulated,* SLATE (Jan. 5, 2015, 2:49 PM), www.slate.com/articles/news_and_politics/view_from_chicago/2015/01/uber_surge_pricing_federal_regulation_over_taxis_and_car_ride_services.single.html; Christian Chessman, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 191 (2017) (describing the high costs of maintaining and updating software).

86. MOAZED & JOHNSON, *supra* note 57, at 170.

The particular characteristics of network effects in such a two–sided market can create particularly high barriers to entry, because they require would–be competitors to scale on both sides of the market in order to succeed. Economist David Evans describes these indirect network effects as follows:

> Multi-sided platforms face a chicken-and-egg problem when they start as a result of what they are trying to accomplish. Consider a platform that is in the business of getting Type As together with Type Bs. Type As may not want to consider the platform unless they know it has attracted Type Bs, but Type Bs may not want to consider the platform unless they know it has attracted Type As. The platform has to figure out a way to get both types of participants on board, in sufficient numbers, to provide value to either.[87]

As dominant platforms continue to gain users, then, the value of their network increases, making it harder to compete with them. As their value increases, moreover, the early mover's existing network makes it more difficult for new entrants to attract venture capital funds.[88] This advantage, then, explains why companies are willing to lose hundreds of millions of dollars—even billions—to scale quickly, outlast their competitors, and create the most powerful network in their respective industry.[89] Uber has already risen meteorically in market valuation and share while one of its two foremost platform competitors, Sidecar, declared bankruptcy. Sidecar's failure can largely be explained by the network effects, which may be especially pronounced in the ridesharing industry where speed and safety are key.[90]

---

87. David Evans, *Multisided Platforms, Dynamic Competition, and the Assessment of Market Power for Internet-Based Firms* (Univ. of Ch. Coase-Sandor Inst. for Law & Econ., Res. Paper No. 753, 2016), http://chicagounbound.uchicago.edu/law_and_economics/799.

88. *How Unicorns Grow*, HARV. BUS. REV., Jan.–Feb. 2016, https://hbr.org/2016/01/how-unicorns-grow.

89. Olivia Zaleski & Lulu Yilun Chen, *Airbnb Said in Talks to Buy China Home-Rental Rival Xiaozhu*, BLOOMBERG (Nov. 23, 2016, 7:40 AM), www.bloomberg.com/news/articles/2016-11-23/airbnb-said-in-talks-to-buy-chinese-home-rental-rival-xiaozhu; *see also* Eric Newcomer, *Uber's Loss Exceeds $800 Million in Third Quarter on $1.7 Billion in Net Revenue*, BLOOMBERG (Dec. 19, 2016, 4:07 PM), www.bloomberg.com/news/articles/2016-12-20/uber-s-loss-exceeds-800-million-in-third-quarter-on-1-7-billion-in-net-revenue.

90. John Ince, *Why Did Sidecar Fail?*, RIDESHARE GUY (Feb. 10, 2016), http://theridesshareguy.com/why-did-sidecar-fail/.

An assessment of whether a platform market is constrained by competition, then, must consider the particularities of lock–in in the context of network effects, including the interdependencies in demand by the participants on both sides of the market. Such interdependencies may indicate pro–competitive constraints, including limiting the price increases or service reductions on one side of the market, lest it affect the service offered to the other; or spurring incremental innovation intended to attract or retain participants on multiple sides in the face of new rivals.[91] Yet they may on the other hand suggest high barriers to entry because new competitors must mobilize two markets.[92]

C. QUESTION THREE: DOES THE PLATFORM'S USE OF THE NETWORK FORM TO COORDINATE TRANSACTIONS CONSTITUTE PRICE FIXING?

Uber's business model involves matching consumers who request rides on a mobile app with individual drivers (some of whom might belong to a larger fleet) willing to provide transport. Uber's model is distinct from the traditional taxi or car–service markets in several ways; optimization algorithms coordinate the matching function, Uber takes a charge for each ride, and the payment is made to the individual driver through the Uber app.[93] The question of the drivers' employment status raises an important vulnerability with regards to antitrust law. In maintaining its position that drivers are independent contractors rather than employees, Uber has opened itself up to the challenge that it has engaged in illegal price fixing by coordinating between millions of independent entrepreneurs to set the same prices, and prohibiting them from competing with one another.

In *Meyer v. Kalanik*, filed in federal district court in New York in 2016, the plaintiff alleged that Uber and its CEO Travis Kalanik violated antitrust law[94] by (1) designing the Uber app, (2) attracting drivers, (3) capturing a significant portion of the market, and (4) mandating ride prices based on "surge pricing"—an algorithm–based variable pricing model based on

91. *See id*.

92. Evans, *supra* note 87.

93. Tim Hwang & Madeleine Clare Elish, *The Mirage of the Marketplace*, SLATE (July 27, 2015, 6:00 AM), www.slate.com/articles/technology/future_tense/2015/ 07/uber _s_algorithm_and_the_mirage_of_the_marketplace.html.

94. The plaintiffs specifically allege that Uber engaged in an illegal scheme to fix prices and thereby injure customers in violation of Section 1 of the Sherman Antitrust Act and Section 340 of New York General Business Law. First Amended Complaint ¶ 1, Meyer v. Kalanick, 174 F. Supp. 3d 817 (S.D.N.Y. 2016) (No. 1:15 Civ. 9796 (JSR)), 2016 WL 950376.

proprietary technology that measures supply and demand at the moment a ride is requested.[95] The lawsuit claims that Uber drivers, unable to opt in or out of surge pricing, are not bidding with each other for the price of a ride. If they were, prices would be driven down.[96] In early 2016, the lawsuit survived a motion to dismiss brought by the defendants.[97] U.S. District Judge Jed Rakoff, presiding over the case, explained that "the fact that Uber goes to such great lengths to portray itself—one might even say disguise itself—as the mere purveyor of an 'app' cannot shield it from the consequences of its operating as much more."[98]

Section 1 of the Sherman Antitrust Act prohibits "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States."[99] To establish a prima facie case for an illegal restraint of trade, a plaintiff must allege 1) some form of concerted action by 2) two or more persons that 3) unreasonably restrains interstate commerce.[100] An illegal restraint of trade can be illegal per se or illegal under the rule of reason.[101] Conduct is per se illegal when the "defendant's actions are so plainly harmful to competition and so obviously lacking in any redeeming pro-competitive values that they are 'conclusively presumed illegal without further examination.'"[102] Horizontal price fixing, a restraint agreed upon by direct competitors, is generally deemed illegal per se.[103]

95. *Id.* ¶ 2–5.

96. Erik Larson & Patricia Hurtado, *Uber Surge-Pricing Antitrust Suit Green-Lighted by Judge*, BLOOMBERG TECH. (Mar. 31, 2016, 3:20 PM), www.bloomberg.com/amp/news/articles/2016-03-31/uber-antitrust-lawsuit-over-pricing-green-lighted-by-judge

97. Jacob Gershman, *Uber Antitrust Lawsuit Clears Court Hurdle in New York*, WALL ST. J. (Apr. 1, 2016, 8:20 PM), http://blogs.wsj.com/law/2016/04/01/uber-antitrust-lawsuit-clears-court-hurdle-in-new-york/.

98. Meyer v. Kalanick, 174 F. Supp. 3d 817, 826 (S.D.N.Y. 2016).

99. 15 U.S.C. § 1 (2012); Zachary C. Flood, *Antitrust Enforcement in the Developing E-Book Market: Apple, Amazon, and the Future of the Publishing Industry*, 31 BERKELEY TECH. L.J. 879, 880–81 (2016).

100. *In re* NASDAQ Market-Makers Antitrust Litig., 894 F. Supp. 703, 710 (S.D.N.Y. 1995); *see also* Kristelia A. García, *Facilitating Competition by Remedial Regulation*, 31 BERKELEY TECH. L.J. 183, 230 (2016).

101. Capital Imaging Assocs., P.C. v. Mohawk Valley Med. Assocs., Inc., 996 F.2d 537, 542 (2d Cir. 1993).

102. *Id.*

103. *Id.*; Leegin Creative Leather Prods., Inc. v. PSKS, Inc., 551 U.S. 877, 886 (2007) ("Restraints that are per se unlawful include horizontal agreements among competitors to fix prices.").

In the alternative, a plaintiff can prove that illegal conduct led to antitrust injury under the rule of reason.[104] Under the rule of reason, the factfinder must balance the benefits of the practice against the harms to consumers.[105] The standard thus examines the actual adverse effect of the alleged anticompetitive behavior on the market as a whole, requiring proof of market injury, and weighs it against the procompetitive 'redeeming virtues' created by the combination of actors, after which the plaintiff can rebut with evidence that the same ends could be achieved with less restrictive means.[106] Most antitrust harms are evaluated using the rule of reason, as most alleged illegal antitrust conduct falls outside of the narrowly prescribed categories that exist for per se violations.[107] Vertical price fixing, in which a principle and a number of subordinate contracting parties agree to an identical restraint that has the effect of price–fixing, is evaluated using the rule of reason.[108]

Uber's method of pricing and fee adjustment makes it vulnerable to both horizontal and vertical price fixing claims, which is what the plaintiffs in *Meyer v. Kalanik* have seized upon. In the preliminary proceedings, the court determined the plaintiff sufficiently alleged both methods of price fixing against Uber.[109] According to the lawsuit, the horizontal price fixing begins when Uber drivers agree to start driving for the service.[110] Uber drivers must sign a written agreement, accept riders using the Uber app, and use the app to collect fees that are determined by Uber's pricing algorithm.[111] Adherence to a universal model of pricing acts as a guarantee that other Uber drivers cannot undercut each other or the company.[112] During "surge times," Uber raises prices because driver supply is lower than rider demand, resulting in up to ten times the fare price.[113] By disallowing drivers from setting their own rates, the plaintiffs allege Uber causes supracompetitive pricing.[114] The plaintiffs further claim that Uber drivers and executives have met at different points to negotiate the increases in

104. *Capital Imaging*, 996 F.2d at 543.
105. *Id.*
106. *See id*.
107. *Id.*
108. Meyer v. Kalanick, 174 F. Supp. 3d 817, 822 (S.D.N.Y. 2016).
109. *Id.* at 822, 825.
110. *Id.* at 824.
111. *Id.*
112. *Id.*
113. *Id.*
114. *Id.*

fares, these increases were to the obvious benefit of Uber and its drivers, and that the increases imply a "common motive to conspire."[115]

In the preliminary hearings, the court was unpersuaded by Uber's argument that contracts between drivers and Uber could not evince a horizontal antitrust conspiracy because each contract was between an individual driver and Uber, and drivers made the decision to join the platform because it was individually in their best interests to do so.[116] The court recognized that "[a]cceptance by competitors, without previous agreement, of an invitation to participate in a plan, the necessary consequence of which . . . is restraint of interstate commerce, is sufficient to establish an unlawful conspiracy under the Sherman Act."[117] Thus, the court found that plaintiffs had met their pleading burden on the claim of horizontal price fixing.[118]

In addition to the claims regarding horizontal price fixing, the *Meyer* plaintiffs alleged that Uber is engaging in vertical price fixing. As described above, while a horizontal price fixing conspiracy is per se illegal under the Sherman Act, vertical price fixing arrangements must be evaluated using the rule of reason.[119] For this claim to defeat a motion to dismiss, the plaintiff must identify a particular market and allege a particular effect on the market by the defendant's conduct.[120] The *Meyer* plaintiffs were specific and narrow in delineating the market: "the mobile app-generated ride-share service market," of which Uber controls eighty percent—which was sufficient for pleading purposes.[121] The court assessed that effect on the

115. *Id.*

116. *See id.*

117. Interstate Circuit v. United States, 306 U.S. 208, 227 (1939); *see also* United States v. Apple, Inc., 791 F.3d 290, 314 (2d Cir. 2015) ("[C]ourts have long recognized the existence of 'hub-and-spoke' conspiracies in which an entity at one level of the market structure, the 'hub,' coordinates an agreement among competitors at a different level, the 'spokes.'"); Laumann v. Nat'l Hockey League, 907 F. Supp. 2d 465, 486–87 (S.D.N.Y. 2012) ("[W]here parties to vertical agreements have knowledge that other market participants are bound by identical agreements, and their participation is contingent upon that knowledge, they may be considered participants in a horizontal agreement in restraint of trade.").

118. *See Meyer*, 174 F. Supp. at 822.

119. *Id.*

120. *See Capital Imaging Associates*, 996 F.2d at 543.

121. *Meyer*, 174 F. Supp. 3d at 821. It is very possible this point will be one of heavy contention as litigation continues—why should the ridesharing market be separated from traditional taxis and car services? Though the court accepted the plaintiffs' contention that the identified market is distinct from the larger market because of the additional amenities

market was sufficiently pled as well.[122] Uber's market position is alleged to have forced Sidecar—an Uber competitor that folded in late 2015—out of the rideshare market, and Uber's dominance is alleged to have prevented new market entrants from emerging.[123]

The fact that the platform model's success involves the use of networks rather than more traditional hierarchical forms of organization, then, implicates the question of whether it might run afoul of traditional antitrust prohibitions on price fixing. More broadly, it has implications for whether application of those principles to this context might correctly be understood as curbing anticompetitive conduct, or whether such an understanding hinders desirable innovation in market organization.

D. QUESTION FOUR: IS THE PLATFORM'S USE OF DIGITAL PRICING ANTICOMPETITIVE?

Digital pricing has been hailed as "the future."[124] More and more companies are using digital algorithms to set prices.[125] In a range of industries, companies use algorithm–based programs to determine what prices should be implemented.[126] Pricing bots are far more accurate and require much less manpower to comprehend current market demands.[127] Given the structure of the platform as a multisided peer network, which means that both supply and demand are highly elastic, dynamic pricing can

(lack of need for cash or card, ability to rate drivers, ability to summon drivers by pressing a button on the app) these differences are, in our estimation, superficial because the identified market provides services that satisfy the purpose of the larger market, the differences are only that of degree rather than kind. The plaintiffs also claimed that Uber is different because traditional cars for hire must be scheduled in advance—this is less true with changes in product offerings by Uber. *Id.* In spite of this potential deficiency in argument, Uber has captured between fifty and seventy percent of business customers in "all types of rides" across all markets, which in and of itself supports an antitrust claim. *See* Thomas M. Jorde & David J. Teece, *Innovation, Cooperation & Antitrust*, 4 BERKELEY TECH. L.J. 1, 45–46 n.118 (1989) (collecting cases where majority market share across all markets supported an antitrust claim).

122. *Meyer*, 174 F. Supp. 3d at 828.

123. *Id.* at 821.

124. James Surowiecki, *In Praise of Efficient Price Gouging*, MIT TECH. REV. (Aug. 19, 2014), http://www.technologyreview.com/review/529961/in-praise-of-efficient-price-gouging/.

125. *See* Dylan I. Ballard & Amar S. Naik, *Algorithms, Artificial Intelligence, and Joint Conduct*, COMPETITION POLICY INT'L 2–3 (May 15, 2017), https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/CPI-Ballard-Naik.pdf.

126. *See id.* at 2.

127. *See id.*

not only match supply and demand, but also operates to increase supply when demand is high: drivers turn on their Uber app when they see that the rates have increased.[128] One recent study has claimed that Uber's pricing algorithm based on demand elasticity generated $6.8 billion of consumer surplus in 2015 alone, suggesting its tremendous pro–competitive capacity.[129] Yet the use of digital algorithms in this fashion also raises two concerns: whether the coordination between pricing bots constitutes tacit collusion that eliminates incentives to compete on price, as well as concerns about platforms' capacity to engage in practices approaching "first–order," or "perfect," price discrimination,[130] by which a firm personalizes prices to reflect the maximum an individual is willing to pay.[131]

1. Does a Digital Platform's Use of Pricing Bots Constitute Illicit Tacit Collusion, and Create Additional Barriers to Competition on Price?

Uber's reliance on digital algorithms for pricing has been met with litigation as well as broader public hostility. And scholars have begun to identify ways that pricing bots used by marketplace platforms can have significant anticompetitive effects.[132] As Ariel Ezrachi and Maurice Stucke explain:

> Uber drivers don't compete among themselves over price . . . Uber's algorithm determines your base fare and when, where, and for how long to impose a surcharge. This by itself is legal. But as the platform's market power increases, this cluster of similar

128. *See* Bill Gurley, *A Deeper Look at Uber's Dynamic Pricing Model*, ABOVE THE CROWD (Mar. 11, 2014), http://abovethecrowd.com/2014/03/11/a-deeper-look-at-ubers-dynamic-pricing-model/.

129. Peter Cohen et al., *Using Big Data to Estimate Consumer Surplus: The Case of Uber* 5 (Nat'l Bureau of Econ. Research, Working Paper No. 22627, 2016), http://www.nber.org/papers/w22627.

130. Ariel Ezrachi & Maurice E. Stucke, *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, 2017 U. ILL. L. REV. 1775, 1807 (2017); Stucke & Ezrachi, *supra* note 78.

131. *See generally* Benjamin Reed Shiller, First-Degree Price Discrimination Using Big Data (Apr. 25, 2014) (unpublished manuscript), https://www.gsb.columbia.edu/faculty-research/sites/faculty-research/files/finance/Industrial/Ben%20Shiller%20--%20Nov%202014_0.pdf (describing the potential for use of big data to engage in such price discrimination).

132. *See, e.g.*, *id.*; Maurice E. Stucke & Ariel Ezrachi, *How Pricing Bots Could Form Cartels and Make Things More Expensive*, HARV. BUS. REV. (Oct. 27, 2016), https://hbr.org/2016/10/how-pricing-bots-could-form-cartels-and-make-things-more-expensive.

> vertical agreements may beget a classic hub-and-spoke conspiracy, whereby the algorithm developer, as the hub, helps orchestrate industry-wide collusion, leading to higher prices . . . . With each algorithm sharing a common interest (profits) and common inputs (similar data), the industry-wide use of algorithms may lead to durable tacit collusion among many competitors.[133]

Similarly, the plaintiffs in *Meyer* contend that Uber's pricing algorithm "artificially manipulates supply and demand by imposing . . . surge pricing on drivers who would otherwise compete against one another on price." All of Uber's partner drivers agree to charge the fare determined by Uber's pricing algorithm. The plaintiffs thereby allege that the drivers entered into horizontal agreements to charge the same prices, and that this horizontal agreement is coordinated vertically by Uber.[134]

While it may appear that algorithms could enhance consumer welfare by causing competitive price reductions at a faster rate, Ezrachi and Stucke demonstrate the way that the speed of algorithmic information–sharing can reduce incentives for competition altogether.[135] Stucke points to the example of a German software app that tracks gas–station prices. Because the algorithm detects price cuts immediately, competitors are able to match the lower price before consumers have time to patronize the discounter, eliminating any motivation for competition on price.[136] When data gets so comprehensive, and analytics so precise, they can accord incumbent competitors what Ezrachi and Stucke call the "God View" of the state of the market at a particular time (adopting Uber's term for the company's tool

133. *Id.*

134. Meyer v. Kalanick, 174 F. Supp. 3d 817, 824 (S.D.N.Y. 2016). A separate lawsuit against Uber was filed in 2016 in Texas, in which the plaintiff alleged that Uber "concocted a plan to fix prices among Uber drivers and then take a percentage of these fares paid by Plaintiff . . . ." Plaintiff's Original Complaint ¶ 1, Swink v. Uber Techs., Inc., No. 4:16-cv-01092, 2016 WL 1620432 (S.D. Tex. Apr. 22, 2016). The plaintiff alleged that the price fixing scheme violated federal antitrust laws as well as Texas antitrust laws. This lawsuit similarly alleged that through the pricing algorithm and its surge pricing component, Uber artificially set the fares for its drivers. The case was resolved when the plaintiff filed a notice of non–suit, and the complaint was dismissed without prejudice. Swink v. Uber Techs., Inc., No. 4:16-cv-01092 (S.D. Tex. July 25, 2016).

135. *See* ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY 72–73 (2016); *see also* David J. Lynch, *Policing the Digital Cartels*, FIN. TIMES (Jan. 8, 2017), www.ft.com/content/9de9fb80-cd23-11e6-864f-20dcb35cede2 (interviewing Stucke).

136. *See* Lynch, *supra* note 135.

permitting it to view the location of all of its drivers and riders).[137] At that point, "computers can anticipate and react to competitive threats well before any pricing change."[138] At this point, ironically, the very market transparency that previously would have fostered competitive behavior would permit algorithms to share price information so quickly that consumers would not be aware of the competition in the first place.[139]

In the case of Uber, then, pricing bots might not just preclude competition on price between individual drivers. The effect of algorithmically–driven price setting could reduce the incentive for competitors to the platform itself—both those already in the market, or those seeking entry—from competing on price altogether. A platform's use of digital pricing thus presents a variety of new challenges for existing antitrust law frameworks, and for policymakers seeking to assess the dimensions of platform market power. Antitrust, especially in assessing a claim of collusion, assumes a human actor, including "[c]oncepts of intent, fear, and 'meeting of the minds' [which] presuppose quintessentially human mental states; they may prove less useful in dealing with computer software and hardware,"[140] and the form of tacit collusion that pricing bots can produce.

Moreover, the traditional inquiry into whether, even if "collusion" might be attributed to bot–driven pricing determinations, "they may nonetheless be so efficient that their benefits outweigh their harms"[141] may be insufficient to capture digital pricing's broader effects on the ability to compete on price in an era of big data and powerful algorithms.

Under current frameworks, regulators would have to assess whether the business model of the platform, including reliance on a pricing bot, "reduce[s] marginal cost even while they make tacit collusion and pricing to consumers above marginal cost more likely; the problem becomes a question of weighing the expected value of positive and negative effects."[142]

---

137. EZRACHI & STUCKE, *supra* note 135, at 72.

138. *Id.* at 73.

139. *See* Lynch, *supra* note 135.

140. Salil K. Mehra, *Antitrust and the Robo-Seller: Competition in the Time of Algorithms*, 100 MINN. L. REV. 1323, 1352 (2016); *see also* Lynch, *supra* note 135 ("Particularly in the case of artificial intelligence, there is no legal basis to attribute liability to a computer engineer for having programmed a machine that eventually 'self-learned' to co-ordinate prices with other machines.").

141. Mehra, *supra* note 140, at 1373.

142. *Id.*

Yet a move towards "perfect" markets suggests caution in the face of uncertainty. One commentator, discussing concerns about the potential for anticompetitive effects in Google's behavior, noted:

> Economic complexity and ambiguity, coupled with an insufficiently deferential approach to innovative technology and pricing practices in the most relevant case law, portend a potentially erroneous—and costly—result. . . . The point is not that we *know* that Google's conduct is procompetitive, but rather that the very uncertainty surrounding it counsels caution, not aggression.[143]

In short, the relevant market dynamics are developing as the platforms—and their underlying technologies—also do so. In recognition of that reality, regulators should be attentive both to the benefits of regulation, and to the potential for unduly stifling beneficial innovation.

2. Does Digital Pricing Permit Unfair Price Discrimination?

Beyond claims that pricing bots can enable collusion, Uber's surge pricing model has been criticized as exploitative of consumer's willingness to pay more in times of bad weather or increased demand.[144] A consistent argument against the introduction of surge pricing by Uber has been the consumer confusion around the actual pricing scheme.[145] Uber has attempted to address this concern. In June 2016, it announced that it is switching from the murky pop ups on the app that tell consumers about surge fares with a multiplier calculation—for example "2.1x" the normal rate—to detailing the dollar amount that will be charged for the ride.[146] "No math and no surprises," as Uber reps stated about the change.[147]

143. 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, 172 (2011).

144. *See* Sanjukta Basu, *Surge Pricing Is Unfair, Unethical and Unconstitutional*, HUFFINGTON POST (July 15, 2016, 8:26 AM), http://www.huffingtonpost.in/sanjukta-basu/surge-pricing-is-unfair-u_b_9739132.html.

145. *See* Utpal M. Dholakia, *Everyone Hates Uber's Surge Pricing – Here's How to Fix It*, HARV. BUS. REV. (Dec. 21, 2015), https://hbr.org/2015/12/everyone-hates-ubers-surge-pricing-heres-how-to-fix-it.

146. *See* Sarah Buhr, *Uber Switches Out Surge for Price Transparency*, TECHCRUNCH (June 23, 2016), https://techcrunch.com/2016/06/23/surgepurge/.

147. *Id.*

Yet, even with these changes, the lack of transparency in algorithmic pricing regimes may mask far more serious anticompetitive effects.[148] Commentators have recently described a nightmarish scenario in which algorithmic pricing, used by a platform with market dominance and the capacity to amass significant personal data about individual consumers, could engage in behavior that could approach perfect price discrimination: person–specific pricing, that charges each user their "exact reservation price"—the maximum they would pay.[149]

Until now, concern for broad–based first–order price discrimination[150] has largely been theoretical because information about an individuals' reservation prices was unobtainable as a practical matter.[151] Yet the advent of big data and analytics offers firms the ability to collect much more precise information on individuals' willingness to pay, raising concerns among policymakers at the highest levels of the Obama White House regarding the implications of increasingly–perfect price discrimination for both fairness and consumer protection.[152]

In contrast to most businesses, platforms now have access to massive amounts of personally–identifiable relevant information. Uber, for example, is in possession of information about a consumer's home (and how much it is worth), place of employment, and schedule (and whether one is later in taking a repeated ride than usual). Uber also has data on patterned behavior regarding which ride offers were previously accepted and which were not, as well as information about a specific destination which may reveal the urgency of the trip.

Indeed, the anti–competitive implications of personalized pricing can become significant as both a platform's market dominance and its access to additional granular personal increases. By discriminating on price in such a way that reflects granular knowledge of individual users' reservation

148. *See* Ryan Cooper, *How Uber Could Become a Nightmarish Monopoly*, WEEK (Feb. 9, 2017), http://theweek.com/articles/675434/how-uber-could-become-nightmarish-monopoly.

149. *See* Cooper, *supra* note 148; Shiller, *supra* note 131.

150. Bracha & Syed, *supra* note 60, at 239 ("Perfect price discrimination is the ability to charge each consumer exactly the price s/he is willing and able to pay for the relevant good.").

151. *See* Shiller, *supra* note 131.

152. EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND DIFFERENTIAL PRICING (2015), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf

values, a firm gains the capacity to capture all available consumer surplus for itself.

Existing competition law provides little guidance for considering the desirability of this behavior. The Robinson–Patman Act of 1936,[153] which deals with price discrimination, applies only to the sale of identical goods—essentially, commodities.[154] Moreover, proposals to expand limits on price discrimination have been rejected on the grounds that such measures would artificially maintain prices above the market level, undercut competition on price, and create barriers to new market entrants.[155] As platforms' digital pricing technology both charges rates that approach individual consumers reservation price and limits the viability of competition on price, policymakers will have to identify new legal frameworks—within and outside traditional antitrust frameworks—to assess the implications for market power and consumer welfare, and address resulting concerns.

E. QUESTION FIVE: DOES THE PLATFORM'S BUSINESS MODEL INVOLVE PREDATORY PRICING?

The benefits accrued by achieving early dominance in a platform market make it crucial that policymakers address the issue of as to whether firms adopted legitimate pricing schemes to fuel network growth, or whether they engaged in anticompetitive predation. A firm engaged in predatory pricing first lowers its price until it is below the average cost of its competitors.[156] Weaker rivals are then forced to sell at a loss, and ultimately leave the market. In the absence of competition, then, the predatory firm raises its price, recouping its loss, and earning monopoly profits thereafter.

Concerns about predatory pricing have been raised frequently in the platform context. The "growth first, revenue later" strategy articulated by Jeff Bezos has successfully fueled Amazon's legendary expansion across markets, supported by venture capital funding in the absence of profits. Consistent with this model, although Uber's user network has grown dramatically, it is not yet profitable. In fact, in the first three quarters of

153. Pub. L. No. 74-692, 49 Stat. 1526 (codified at 15 U.S.C. § 13 (2012)).

154. *See* Cooper, *supra* note 148 (noting that such behavior would not run afoul of the Robinson–Patman Act, which governs only commodities).

155. AM. BAR ASS'N SECTION ON ANTITRUST LAW, 1 THE ROBINSON-PATMAN ACT: POLICY AND LAW 27–31 (Paul H. LaRue et al. eds., 1980).

156. *See* David S. Evans, *Governing Bad Behavior by Users of Multi-Sided Platforms*, 27 BERKELEY TECH. L.J. 1201, 1244 (2012) (describing the process of predatory pricing as applied by courts).

2016, Uber lost more than $2.2 billion. And just as Amazon was criticized for engaging in a combination of below–marginal–cost sales and new infusions of venture funding as a means of achieving scale and market power at the expense of competitors, Uber's lack of profitability has raised claims of predatory pricing.[157]

Current legal standards governing predation claims suggest ambivalence about the cause of action,[158] and raise a high bar for success. The Supreme Court has expressed doubt as to the frequency of engagement in predatory practices, and its belief in the irrationality of pursuing such a strategy.[159] Reflecting these understandings, the Court, in the 1993 case of *Brooke Group v. Brown & Williamson Tobacco,*[160] required plaintiffs pursuing predation claims not only (1) to establish that the below–cost pricing was capable of "producing the intended effects on the firm's rivals," but also (2) to demonstrate "a likelihood that the predatory scheme alleged would cause a rise in prices above a competitive level that would be sufficient" to allow the defendant to recoup its losses.[161] Under this high evidentiary threshold, the Federal Trade Commission has not successfully brought a predatory pricing case since that year.

Policymakers assessing platform market power will accordingly face an important decision regarding how to view predatory pricing in a two–sided digital market. In particular, they will increasingly need to consider whether the interaction between a platform's below–cost pricing and other attributes of platform markets that have shaped the competition landscape counsel a more lenient standard for claims that predatory pricing injured competition. This Essay has explored the suggestion, discussed above, that achieving a "critical mass" of users on both sides of a platform's market quickly is necessary to become one of the entrenched incumbents, and to enjoy the power of network effects in strengthening the resulting market dominance. In a context with such robust advantages for incumbents, prioritizing growth over profits and the resort to below–cost pricing to achieve

157. *See supra* note 33.

158. *See* Christopher J. Leslie, *Predatory Pricing and Recoupment*, 113 COLUM. L. REV. 1695, 1698 (2013) ("Predatory pricing has long been a controversial cause of action in antitrust."); Evans, *supra* note 156, at 1244.

159. *See* Brooke Grp. v. Brown & Williamson Tobacco, 509 U.S. 209 (1993); Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 589 (1986) ("[P]redatory pricing schemes are rarely tried, and even more rarely successful.").

160. 509 U.S. 209 (1993).

161. *Brooke Grp.*, 509 U.S. at 226.

substantial market share quickly may be much more rational than the Court's precedents would suggest.[162] This fact might prompt policymakers to consider whether, in light of the characteristics of a particular platform's market model, anticompetitive concerns are exacerbated or whether strong network effects in a two–sided markets counsel more stringent standards regarding competitive injury. Policymakers should also consider whether predation might occur even when a firm does not operate below costs, but instead relies on an asymmetric pricing scheme that lowers prices significantly on one side of the market to promote user growth. Such a scheme could create network effects that raise switching costs, and the ability to charge higher prices, on the other side of the market.[163]

F. QUESTION SIX: DOES THE PLATFORM'S COLLECTION AND USE OF DATA RAISE OR EXACERBATE ANTICOMPETITIVE CONCERNS?

Companies across all industries are increasingly using information collected about customer interactions in order to improve their operations. This is especially true on the digital platform, where consumer data is easily collectible and the technology to mine this information is rapidly advancing.[164] As we have seen throughout the inquiries regarding platform market power, big data and analytics are core elements of the platform business model.[165] At the same time, the massive amounts of information that can be collected and used about users on the platform raises concerns about potential new anticompetitive practices. In 2015, the Federal Trade Commission created the Office of Technology Research and Investigation designed in part to investigate these questions.[166] Specifically, the Commission is examining "the ways that firms compete using big data as a product, an input, or a tool for making competitively significant

162. Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 564, 564 (2017).

163. Amelia Fletcher, *Predatory Pricing in Two-Sided Markets: A Brief Comment*, 3 COMPETITION POLICY INT'L 221 (2007); *see also* MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 189 (2016) (discussing the "spill-over" network effects from one side of a market to another).

164. *Id.*

165. *Id.*

166. Jessica Rich, *BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection*, FED. TRADE COMM'N (Mar 23, 2015, 2:01 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/03/bcps-office-technology-research-investigation-next/.

decisions."[167] The major antitrust concerns surround the control of data by a small number of concentrated companies and the lack of transparency about their collection and usage.[168]

Scholars and regulators are engaged in ongoing debates over the relationship between big data and competitiveness. Some maintain that the collection and possession of big data does not offer a firm a comparative competitive advantage.[169] These scholars argue that data is both imitable and nonrivalrous, and thus new market entrants face low barriers to replicating it.[170]

Yet the view among both regulators and many scholars is that the data held by a platform—especially one with a large market share—can both be used to limit competition and to harm consumers. For example, in 2014 the European Commission considered the effect on competition in the online advertising market of combining user data, in reviewing Facebook's acquisition of WhatsApp.[171] The Commission ultimately permitted the merger, citing the existence of numerous competitors possessing their own collections of user data, but the inquiry recognized the danger.[172] Subsequently, EU competition commissioner Margrethe Vestager explained that the Commission would frown upon businesses that restrict others' access to "unique" data, explaining:

> We shouldn't be suspicious of every company which holds a valuable set of data. But we do need to keep a close eye on whether companies control unique data, which no one else can get hold of, and can use it to shut their rivals out of the market. That could

167. Shepard Goldfein & James A. Keyte, *Antitrust and 'Big Data': New Terrain for Inquiry?*, N.Y. L.J. (Mar. 7, 2016), www.newyorklawjournal.com/id=1202751429490/Antitrust-and-Big-Data-New-Terrain-for-Inquiry.

168. Rich, *supra* note 166.

169. *See* Anja Lambrecht & Catherine E. Tucker, Can Big Data Protect a Firm from Competition? (Dec. 18, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2705530.

170. *See* STUCKE & GRUNES, *supra*, note 163, at 42 (responding to such claims as set forth in Darren S. Tucker & Hill B. Wellford, *Big Mistakes Regarding Big Data*, ANTITRUST SOURCE 7 (Dec. 2014), https://www.americanbar.org/content/dam/aba/publishing/antitrust_source/dec14_tucker_12_16f.authcheckdam.pdf.

171. Press Release, European Comm'n, Mergers: Commission approves acquisition of WhatsApp by Facebook (Oct. 3, 2014), http://europa.eu/rapid/press-release_IP-14-1088_en.htm.

172. *Id.*

> mean, for example, data that's been collected through a monopoly.[173]

Indeed, OECD recently concurred with the notion data–driven markets "can lead to a 'winner takes all' result where concentration is a likely outcome of market success."[174] The result of platform–winner–takes–all is further supported by a recent study in the Harvard Business School. In the study, researchers scored companies seeking venture capital funding on the basis of whether they were attempting to create entirely new categories of products or services, and whether they are "cultivating large and active developer ecosystems, among other criteria."[175] The study concluded that:

> the vast majority of post-IPO value creation comes from companies call[ed] "category kings," which are carving out entirely new niches; think of Facebook, LinkedIn, and Tableau. Those niches are largely "winner take all"—the category kings capture 76% of the market.[176]

Uber collects a massive amount of data, including both personal information and the information about traffic, travel times, and market demand that power its algorithms. It has recently announced its intention to make some of that data—information about traffic and transit times—available to urban planners and the public through a new website, Uber Movement.[177] Yet, as previously mentioned, the type of data that it does not intend to share—including the personal consumer data, as well as ranking and review information—has an impact on a range of competition issues. These include enabling the possibility of anticompetitive price discrimination, and exacerbated lock–in effects by personalizing the platform experience, enhancing the value of review systems, and targeting services. More generally, Uber's scale and market position suggests that it

---

173. Margrethe Vestager, Comm'r on the European Comm'n, Making Data Work for Us (Sept. 9, 2016), https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/making-data-work-us_en

174. Maurice E. Stucke & Allen P. Grunes, *Debunking the Myths Over Big Data and Antitrust* (Univ. of Tenn. Legal Studies, Research Paper No. 276, 2015), http://ssrn.com/abstract=2612562.

175. HARV. BUS. REV., *supra* note 88.

176. *Id.*

177. *Uber Movement FAQs*, UBER, https://movement.uber.com/faqs?lang=en-US (last visited Nov. 8, 2017); *see also* Dom Galeon, *Uber Releases a Staggering 2 Billion Trips-Worth of Traffic Data*, FUTURISM (Jan. 11, 2017), https://futurism.com/uber-releases-a-staggering-2-billion-trips-worth-of-traffic-data/.

would be difficult for new entrants to gather the amount of data Uber has already collected and which shapes Uber's algorithms. And as suggested below, the possession of "big data" can facilitate the leveraging of market dominance to new markets.

There may be wide–ranging ways that Uber and other two–sided platforms can abuse their market power by taking advantage of the massive data they collect, to the detriment of both sides of the market.[178] Because of its role as intermediary, Uber has access to significant data unavailable to both drivers and riders, and a capacity to monitor which is not reciprocally available to either group. By means of this information asymmetry, the platform can leverage "access to information about users and their control over the user experience to mislead, coerce, or otherwise disadvantage sharing economy participants"—a claim reflected in the revelation of Uber's manipulation of drivers to increase supply during times that would benefit the platform.[179]

Additionally, in the digital context, "increased market usage and share" can correlate with "increased quality"[180]—what Maurice Stucke and Allen Grunes call "learning–by–doing" network effects. They argue that "as more people use the search engine and the more searches they run, the more trials the search engine's algorithm has in predicting consumer preferences, the more feedback the search engine receives of any errors, and the quicker the search engine can respond with recalibrating its offerings."[181] Thus, platform related lock–in effects may have certain socially beneficial outcomes that regulators should consider alongside the risks to competition.

Regulators have already begun to consider the ways that collection of the data shared by with platforms by users can foreclose competition. Recognizing that big data will be a lasting force in competition analysis, the OECD's Competition Committee offered several salient approaches that policymakers might use when engaging in this inquiry.[182]

178. Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623, 1624 (2017).

179. Noam Scheiber, *How Uber Uses Psychological Tricks to Push Its Drivers' Buttons*, N.Y. TIMES (Apr. 2, 2017), www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html.

180. STUCKE & GRUNES, *supra* note 163, at 174.

181. *Id.* at 175.

182. ORG. FOR ECON. COOPERATION & DEV., SUMMARY OF DISCUSSION OF THE HEARING ON BIG DATA (2016), https://one.oecd.org/document/DAF/COMP/M(2016)2/ANN2/FINAL/en/pdf.

First, the Committee recognized that a platform's possession of users' data can create lock–in effects by increasing switching costs, and raising barriers to entry. Accordingly, they proposed that "[c]ompetition authorities should then carefully examine on a case-by-case basis to what extent business performance depends on the ability to collect data; evaluate the degree of substitutability between different datasets; and identify the amount of data required for an entrant to compete."[183]

Second, the Committee offered two ways for thinking about data, and how current legal analysis might respond to the big data challenge. Their discussion suggested on the one hand "that it may be enough to adapt existing tools" when considering big data as corporate asset in a competition analysis. On the other hand, "there is more work to do in order to incorporate data as a quality/performance issue into competitive analysis," involving questions like lock–in.[184] Policymakers should bear both of these considerations in mind when fashioning oversight for platforms.

G. QUESTION SEVEN: IS THE PLATFORM LEVERAGING ITS MARKET POWER UNFAIRLY TO ESTABLISH A DOMINANT POSITION IN OTHER MARKETS?

In 2017, *Vanity Fair* combined its two lists of the "New Establishment"—"The Disrupters," dedicated to Silicon Valley upstarts, and "The Powers That Be," dedicated to the financial and entertainment moguls of New York and Los Angeles. The magazine explained that combining the list fits with what competition looks like today:

> On some level, everyone is now in the technology business . . . . Jeff Bezos may have started out wanting to sell books, but now Amazon is contending with Hollywood, FedEx, and Apple in the entertainment, logistics, and streaming businesses. Kalanick may have initially wanted to make it easier to find a cab, but now Uber is competing in the self-driving-car industry against not only G.M., Chrysler, and Ford but also Tesla and Google, among many others. Spiegel started Snapchat to facilitate the act of sending risqué messages. Four years later his company is a legitimate threat to the entire future of television.[185]

The expansion of market–dominant companies into new markets can offer significant pro–competitive advantages. By moving into new

183. *Id.* at 5.
184. *Id.* at 8.
185. *Id.*

technological spaces and new markets, powerful, well–funded players can offer new sources of disruption and innovation, whether through internal technological innovation and development of capacity to enter new markets, creating market partnerships, or –as is often the case—acquisition of other firms engaged in innovation.

Further, leveraging market power to compete in other markets is often at the very core of the platform business model. In the words of Reid Hoffman, the founder of LinkedIn, the world's largest online professional network platform, "[i]t's about building the next big platform."[186] Indeed, "[o]nce it has gained a foothold . . . the firm raises venture capital and tries to enter bigger markets and grow as quickly as possible."[187]

Uber has been similarly transparent about its goal to leverage its market dominance in the ride–coordination market to pioneer the self–driving automobile market.[188] In a matter of months, it has purchased Otto, a startup that retrofits existing trucks with self–driving technology,[189] and artificial intelligence startup Geometric Intelligence,[190] as well as announced the establishment of Uber AI Labs, a research arm dedicated to artificial intelligence and machine learning.[191] Uber is now the leading player in the driverless car market specifically because of the elements of its market power in the ride–coordination market—notably, its scale, its data, and its access to capital in the absence of profits.[192] Indeed, some have suggested that the only company that can compete in this new market is another platform dominant in adjacent markets—Google.[193]

186. ECONOMIST, *supra* note 56.

187. *Id.*

188. Elizabeth Weise & Marco della Cava, *Uber's Self-Driving Car Ambitions Live Another Day*, USA TODAY (May 4, 2017, 2:12 PM), www.usatoday.com/story/tech/news/2017/05/03/uber-waymo-still-battling-over-details-critical-self-driving-car-tech-suit/101244568/.

189. Romaine Dillet, *Uber Acquires Otto to Lead Uber's Self-Driving Car Effort*, TECHCRUNCH (Aug. 18, 2016), https://techcrunch.com/2016/08/18/uber-acquires-otto-to-lead-ubers-self-driving-car-effort-report-says/.

190. Polina Marinova, *Uber Just Bought a Startup You've Never Heard Of. Here's Why That's Important*, FORTUNE (Dec. 5, 2016), http://fortune.com/2016/12/05/uber-artificial-intelligence-acquisition/

191. *Id.*

192. *See* Daniel Matthews, *Big Data on Wheels: Google vs. Uber in the Driverless Revolution*, SMARTDATACOLLECTIVE (Dec. 23, 2016), www.smartdatacollective.com/daniel-matthews/458204/big-data-wheels-google-vs-uber-driverless-revolution.

193. *See, e.g.*, Jason Abbruzzese, *Uber and Google Do Battle Over Self Driving Car Tech*, MASHABLE (May 20, 2017), http://mashable.com/2017/05/20/uber-vs-google-

Only time will reveal whether Uber, Google, or other innovators will demonstrate the capacity to excel in the driverless transportation market; yet this scenario raises the possibility of a capacity for platforms, with their technological and data–based foundations, to leverage their power into adjacent markets.[194] Antitrust and competition law has long recognized that, in certain limited instances, such leveraging might be anti-competitive.[195] Especially in data–driven platform markets characterized by strong network and lock–in effects—and in new technological contexts that might otherwise be ripe for competitive innovation—policymakers should look hard at whether the aspects of a platform's power combine in a way that threatens to compound losses to consumer welfare.

H. QUESTION EIGHT: DOES THE PLATFORM'S MARKET POWER INAPPROPRIATELY RESTRICT CONSUMER CHOICE ABOUT PERSONAL PRIVACY?

Finally, policymakes must ask whether a platform can exploit market power to unfairly limit consumer choice regarding privacy protections. Remember that network effects and switching costs can constrain competition by locking consumers into using a single platform even when a competitor might compete favorably on product or price. In this context, a competitive offering would need to be substantially more attractive to lure consumers away from the dominant player. Similarly, lock in could eliminate competitive pressure on platforms to improve quality along the privacy–protective dimension—and even offer them substantial leeway to

---

waymo-self-driving-car-wars-get-nasty/ (describing litigation between Google and Uber over driverless car innovation).

194. Lothar Determann & Bruce Perens, *Open Cars*, 32 BERKELEY TECH. L.J. 913, 919 (2017) ("Social media companies may push for a socially connected car—the next platform after the personal computer, smartphone, and virtual reality headset. Companies with strong content portfolios may view the car as a platform to distribute for video and audio material.").

195. *See generally* Int'l Salt Co. v. United States, 322 U.S. 392, 396 (1947) (tying the use of patented products to the use of unpatented products is a per se antitrust violation); Dennis W. Carlton & Michael Waldman, *The Strategic Use of Tying to Preserve and Create Market Power in Evolving Industries*, 33 RAND J. ECON. 194 (2002); Benjamin Edelman, *Does Google Leverage Market Power Through Tying and Bundling?*, 11 J. COMPETITION L. & ECON. 365 (2015). When the Justice Department sued Microsoft Corp in 1998 the lawsuit was aimed at stopping it from using its dominance of the operating system market to also dominate browser software. United States v. Microsoft Corp., 253 F.3d 34, 45 (D.C. Cir. 2001).

adopt significantly less privacy–protective practices without market pushback.

Given the account of Uber's development as a data–driven firm, constraints along this dimension could have significant impact for data protection. Indeed, in the words of one analyst, "we are going to see the transformation of Uber into a big data company cut from the same cloth as Google, Facebook and Visa - using the wealth of information they know about me and you to deliver new services and generate revenue by selling this data to others."[196]

While exploration of the relationship between antitrust and privacy concerns has not fully matured, regulators have begun to address the concern that network effects in platform markets can unfairly constrain consumer privacy choices. In the United States, former FTC Chairman Pamela Jones Harbour first made this case, raising the issue of whether network effects resulting from the two companies' data would deprive consumers of meaningful privacy choices in her dissent to the Commission's 2007 decision to clear the Google/DoubleClick merger.[197] In later writings, Chairman Harbour advocated that privacy should be explicitly integrated into antitrust analysis, by asking in single–firm conduct investigations whether "achieving a dominant market position might change the firm's incentives to compete on privacy dimensions" or reduce incentives to innovate new technologies that would protect consumer privacy.[198] The FTC has since indicated that proposed mergers can be assessed in terms of impact on non–price competition, including competition on privacy protection.[199]

196. Ron Hirson, *Uber: The Big Data Company*, FORBES (Mar. 23, 2015, 9:15 AM), https://www.forbes.com/sites/ronhirson/2015/03/23/uber-the-big-data-company/.

197. *In re* Google/DoubleClick, FTC File No. 071-0170, at 5, 9–12 (Dec. 20, 2007) (Harbour, Comm'r, dissenting), https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf; *see also* James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1131 (2013) (summarizing Chairperson Harbour's writings on the subject).

198. Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769, 794 (2010).

199. Debbie Feinstein, *The Not-So-Big News About Big Data*, FED. TRADE COMMISSION (June 16, 2015, 11:30 AM), https://www.ftc.gov/news-events/blogs/competition-matters/2015/06/not-so-big-news-about-big-data ("[T]he FTC has explicitly recognized that privacy can be a non-price dimension of competition.").

EU regulators have articulated the case even more comprehensively. In 2014, former European Data Protection Supervisor Peter Hustinx, published an Opinion calling for a "holistic approach" to the regulation of data protection, competition and consumer protection laws. [200] His successor, current EDPS Giovanni Buttarelli, has called for the establishment of a "digital clearinghouse"[201] to bring together agencies from the areas of competition as well as consumer and data protection to develop guidelines that articulate "theories of harm relevant to merger control cases and to cases of exploitative abuse" that also reflect both principles of data protection and consumer protection.[202] And in March, 2016 the German Federal Cartel Office announced[203] that it had launched an investigation into whether Facebook may have committed an infringement of Article 102 of the Treaty on the Functioning of the European Union.[204] The allegation is that Facebook has abused its dominant market position by requiring its users to sign up to unfair terms regarding its use of their personal data.[205]

Just as lock–in effects might prevent consumers from adopting more efficient alternatives, in a platform era such competition–constraining consequences might prevent consumers from other choices guaranteed to them, and must be considered in any examination of a platform's market power.

200. EUROPEAN DATA PROT. SUPERVISOR, PRIVACY AND COMPETITIVENESS IN THE AGE OF BIG DATA: THE INTERPLAY BETWEEN DATA PROTECTION, COMPETITION LAW AND CONSUMER PROTECTION IN THE DIGITAL ECONOMY (2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.

201. *Big Data & Digital Clearinghouse*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearing-house_en/ (last visited Aug. 9, 2017).

202. Guy Lougher, *Regulatory Focus on Data Access Restrictions Could Impact Uber, Retailers, Insurers and Car Manufacturers, Says Expert*, OUT-LAW (Sept. 26, 2016), https://www.out-law.com/en/articles/2016/september/regulatory-focus-on-data-access-restrictions-could-impact-uber-retailers-insurers-and-car-manufacturers-says-expert-/.

203. Eric Auchard, *Germany Takes on Facebook in Competition Probe*, REUTERS (Mar. 2, 2016, 1:45 AM), https://www.reuters.com/article/us-facebook-germany-dataprotection/germany-takes-on-facebook-in-competition-probe-idUSKCN0W40Y7.

204. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 102, May 9, 2008, 2008 O.J. (C 115) 89; A. Douglas Melamed, *Antitrust Law Is Not That Complicated*, 130 HARV. L. REV. 163, 169 & n.35 (2017).

205. Auchard, *supra* note 203.

III. CONCLUSION

Identifying information as the world's most valuable resource—and its manipulation and use as a leading source of economic power—commentators have called for a reexamination of both antitrust and regulation in the data economy.[206] This Essay has offered a framework for beginning to identify issues implicating competition, consumer welfare, and market fairness in a platform age. As these questions are framed, the answers will suggest conditions under which traditional legal and regulatory approaches continue to provide appropriate market safeguards. At the same time, unique attributes of the platform economy may suggest contexts in which reworking traditional legal approaches will be necessary. Such doctrinal shifts should be made in light of the types of power achieved through new models of organizations, the use of data and analytics on which platform companies rely, and the durability of economic strength that can result. These remarkable changes have the potential not just to reshape the law within doctrinal categories, but to necessitate a blurring of categories themselves, and a reconsideration of how different legal tools—from competition law, to privacy protection, to other varied regulatory strategies—should best be employed in the digital economy.

206. *See, e.g.*, *The World's Most Valuable Resource Is No Longer Oil, But Data*, ECONOMIST (May 6, 2017), www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource/.

DETERRING CYBERCRIME: FOCUS ON INTERMEDIARIES

Aniket Kesari,[†] Chris Hoofnagle[††] & Damon McCoy[†††]

ABSTRACT

This Article discusses how governments, intellectual property owners, and technology companies use the law to disrupt access to intermediaries used by financially–motivated cybercriminals. Just like licit businesses, illicit firms rely on intermediaries to advertise, sell and deliver products, collect payments, and maintain a reputation. Recognizing these needs, law enforcers use the courts, administrative procedures, and self–regulatory frameworks to execute a deterrence by denial strategy. Enforcers of the law seize the financial rewards and infrastructures necessary for the operation of illicit firms to deter their presence.

Policing illicit actors through their intermediaries raises due process and fairness concerns because service–providing companies may not be aware of the criminal activity, and because enforcement actions have consequences for consumers and other, licit firms. Yet, achieving direct deterrence by punishment suffers from jurisdictional and resource constraints, leaving enforcers with few other options for remedy. This Article integrates literature from the computer science and legal fields to explain enforcers' interventions, explore their efficacy, and evaluate the merits and demerits of enforcement efforts focused on the intermediaries used by financially–motivated cybercriminals.

DOI: https://doi.org/10.15779/Z387M04086

† UC Berkeley School of Law, Jurisprudence & Social Policy.

†† UC Berkeley School of Law & School of Information.

††† New York University Tandon School of Engineering. The author thanks the National Science Foundation under contract 1619620 and a gift from Google for financial support of this project.

The authors thank the Center for Long Term Cybersecurity for financial support of this project, and Laurin Weissinger, Annemarie Bridy, and Zachary Goldman for critical feedback.

TABLE OF CONTENTS

I. INTRODUCTION

Businesses that sell illegal pharmaceuticals, counterfeit goods, or offer computer attacks online have similar goals and needs as ordinary firms. These enterprises must acquire new customers, have a supply chain, maintain a web presence, collect payments, deliver a product or service, and, finally, cultivate a positive reputation to encourage repeat sales. In pursuit of profit, the legitimate and illegitimate alike depend on many third parties, including web hosts, payment providers, and shipping companies.

Licit businesses are deterred from illegal acts by punishment, through fines, threats, and regulatory actions. But enforcers often cannot use traditional deterrence against financially–motivated cybercriminals because law enforcement is limited by scarce resources, competing enforcement priorities, and jurisdictional challenges. As a result, enforcers—both public and private—have turned to deterrence by denial approaches. Such approaches attempt to deter conduct by spoiling, reducing, or eliminating the benefits of computer crime. Frustrated by attempts to reach actual illicit actors, enforcers focus on third parties that are critical to business operation, thus denying cybercriminals' access to banking, web resources, or even shipping services. Cybercrime, often presented as ephemeral and stateless, can be reined in through attacking dependencies critical to its operation.

Much of the legal academic scholarship on Internet intermediaries focuses on intermediaries' general immunity from state law actions under the Communications and Decency Act Section 230 (CDA 230) or the provisions of the Digital Millennium Copyright Act (DMCA). CDA 230 creates broad immunity for Internet intermediaries, insulating them from the illegal acts of their users; intermediaries, even when given notice of noxious content, are not required to remove it.[1] The DMCA can shield providers from liability for user's infringing activities if certain steps are taken to receive and respond to takedown requests by intellectual property (IP) owners.[2]

This Article turns away from the CDA 230 and the DMCA procedures to focus on mechanisms that force intermediaries to address alleged user misbehavior. Specifically, this Article focuses on three mechanisms that are used to cause intermediaries to take or refrain from some action related to financially–motivated cybercrime. Parts II and III set the stage for the survey. Part II canvasses the literature on cybercrime and intermediaries. Part III discusses the business constraints of three kinds of actors: botnet operations, sites that offer illegal and infringing goods, and the contests among intermediaries and intellectual property owners. Part IV covers the use of Rule 65 of the Federal Rules of Civil Procedure (FRCP) and its allowance for broad forms of injunctive relief, and the Domain Name Service takedown procedures that use the U.S. government's ability to target infringing websites and make them inaccessible. Part V covers

1. 47 U.S.C. § 230 (2012).
2. 17 U.S.C. § 512 (2012).

administrative remedies focused on financial services intermediaries. Finally, part VI looks at self–regulatory procedures that intermediaries have established to allow IP owners and governments to block user activity.

An intermediary–focused approach raises due process and fairness concerns because intermediaries may not be privy to criminal activity, and enforcement mechanisms affect consumers and other licit firms. Cybercriminals may mask their behavior by commandeering ordinary users' accounts and computers for attacks and monetization of crimes. Thus, when an enforcer investigates and makes interventions, legal demands may fall upon third parties, individuals, and businesses that were merely used as conduits by the suspect. These intermediaries themselves may have been hacked or otherwise be cybercrime victims themselves. Additionally, compliance may impose costs on intermediaries and to civil society in the form of censorship or erosion of Internet anonymity as intermediaries are asked to know their customers[3] and make requirements that ordinary users provide documentation of their identity. Interventions are done *ex parte*, with surprising speed, raising the risk that others' interests may not be fully considered by a court. Finally, there is always the problem of claimant abuse—claims of wrongdoing may be motivated by anticompetitive interests or simple censorship.

In sum, this Article offers an exploratory look at an understudied area of intermediary interventions. Intermediary liability conversations typically surround CDA 230 and the DMCA, but our survey reveals that intermediaries can be subject to costly, broad interventions in cybercrime contexts. This Article highlights the current legal practices in this space, and evaluates their merits and demerits.

II. LITERATURE REVIEW

This Part highlights relevant literature from both a theoretical and legal perspective, starting with a brief overview of the literature on the economics of financially–motivated cybercrime. These pieces link the economics of cybercrime to the economics of crime more broadly, and identify the features of cybercrime that make it amenable to intermediary interventions. The focus then shifts to the legal theory concerning the

3. Anti–money laundering customer identification requirements are known as "Know Your Customer" regulations. *See* 12 U.S.C. § 635(i) (2012); 31 C.F.R. § 1020.200 et. seq. (2016).

extent to which intermediaries should be held liable, before turning to the implementation of legal rules and interventions.

Some cybersecurity literature focuses on intermediaries' centrality in Internet activity. Authors detail the both private and government policies that aim to thwart cybercrime and create secure systems. Goldman and McCoy set up the motivation for our inquiry in their paper, *Deterring Financially Motivated Cybercrime*.[4] For instance, they address how some cybercriminals are dependent upon a handful of payment processors, which empowers those payment processors to effectively combat criminals.[5] They argue that mainstream payment processors adopt policies that help thwart and deter cybercrime, in large part because payment companies want to maintain the integrity and the reputation of their own systems.[6] This is a boon for the government and potential victims of cybercrime because payment processors can interrupt a large portion of cybercrime without imposing direct costs on consumers.

Cybercrime is an increasingly professional endeavor that implicates activities involving American companies, or are otherwise subject to U.S. courts' jurisdiction. In *The Economics of Online Crime*, Moore et al. elaborate on how cybercrime professionalization lends itself to well-understood policy fixes.[7] They explain that criminal firms have emerged that specialize in botnet creation, phishing, and identity theft.[8] They argue, "[w]ith this new online crime ecosystem has come a new profession: the 'botnet herder'—a person who manages a large collection of compromised personal computers (a 'botnet') and rents them out to the spammers, phisher[s], and other crooks."[9] Because cybercrime has become increasingly professionalized, it has started to look more like conventional crime that has been explored at length in the economics of crime literature.[10]

Beyond payment processors and criminals themselves, another area of this literature focuses on internet infrastructure and its relationship to cybercrime. In *The Turn to Infrastructure in Internet Governance*, the

4. Zachary K. Goldman & Damon McCoy, *Deterring Financially Motivated Cybercrime*, 8 J. NAT'L SECURITY L. & POL'Y 595 (2016).

5. *Id*. at 611–12.

6. *Id*. at 612.

7. *See generally* Tyler Moore, Richard Clayton & Ross Anderson, *The Economics of Online Crime*, 23 J. ECON. PERSP. 3 (2009).

8. *Id.* at 4.

9. *Id.* at 5.

10. *Id*. at 18.

authors look at the fundamental building blocks of the Internet as sources for governance and, consequently, security.[11] For instance, authors discuss the role of the Domain Name System (DNS) and the Internet Corporation for Names and Numbers (ICANN) as the backbones of the Internet.[12] This is important for cybersecurity because of the U.S. government's ability to directly seize domain names and take control of infringing websites, as discussed, in more detail. Essentially, the authors point out that even though the Internet was designed to usher in diffused and ground–up governance, in actuality, governance structures can reduce access to certain resources needed by cybercriminals.[13]

Similarly, in *Holding Internet Service Providers Accountable*, Douglas Lichtman and Eric Posner argue that Internet Service Providers (ISPs) can be essential nodes in cybercrime networks, and should be held to higher legal standards.[14] They argue that the move toward granting immunity to ISPs is ill–advised because it underestimates ISPs' ability to deter cybercrime, and gives them license to allow dangerous behavior.[15] This argument is in line with standard law and economics theory, predicting that always assigning liability to one party (in this case, victims) will cause the other party (in this case, ISPs) to take inefficient levels of precaution.[16] Lichtman and Posner map the theory of indirect liability onto the actions taken by ISPs and conclude that ISPs should share some responsibility for cybercrime.[17]

---

11. THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE (Francesca Musiani, Derrick L. Cogburn, Laura DeNardis & Nanette S. Levinson eds., 2016); *see also* Annemarie Bridy, *Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation*, 74 WASH. & LEE L. REV. 1345 (2017).

12. Musiani, Cogburn, DeNardis & Levinson, *supra* note 11, at 9–10.

13. *Id.* at 11–12; JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).

14. Doug Lichtman & Eric C. Posner, *Holding Internet Service Providers Accountable*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 221, 221–58 (Mark F. Grady & Francesco Parisi eds., 2006).

15. *Id.* at 229–30.

16. ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 199–227 (6th ed. 2016).

17. Lichtman & Posner, *supra* note 14, at 222.

> ISPs should to some degree be held accountable when their subscribers originate malicious Internet code, and ISPs should also to some degree be held accountable when their subscribers propagate malicious code by, for example, forwarding a virus over e-mail or adopting lax security precautions that in turn allow a computer to be co-opted by a malevolent user.

Moving from theory to policy, *Operation Seizing Our Sites* raises criticisms of an overbroad intermediary–centered approach.[18] In the article, Karen Kopel discusses federal programs that aim to take down copyright and trademark infringing websites.[19] In particular, she critiques "Operation In Our Sites," a major government initiative for enforcing stricter IP protections.[20] The program's main mechanism allows the Department of Justice and Immigrations and Customs Enforcement (ICE) to seize domain names by ordering intermediaries to reassign them, and make these resources inaccessible to users who try to access a website through its alphanumeric name.[21] She argues that the process largely circumvents normal procedural safeguards, and grants the government wide discretion in pursuing potential infringers.[22] She also notes the risks associated with the approach, namely that the government has taken legitimate websites offline and offered them few due process protections to appeal the decision.[23] In practice, hardly any websites are able to recover their domains after a government seizure.[24]

The next Part turns to the business constraints that financially–motivated cybercriminals face, and examines those actors' various activities, including their dependence on intermediaries. It then summarizes the legal processes used in situations where enforcers—both public and private—attempt to deter financially–motivated cybercrime by interfering with intermediaries.

III. BUSINESS CONSTRAINTS, RELEVANT ACTORS, AND ACTIVITIES

Financially–motivated cybercriminals face many of the same business constraints and challenges that legitimate enterprises do. A paradigmatic example comes from an illegal goods business called Silk Road, which provided a marketplace for drugs, fake identification documents, and

18. Karen Kopel, *Operation Seizing Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice*, 28 BERKELEY TECH. L.J. 859 (2013); *see also* Annemarie Bridy, *Carpe Omnia: Civil Forfeiture in the War on Drugs and the War on Piracy*, 46 ARIZ. ST. L.J. 683 (2014).
19. Kopel, *supra* note 18 at 862–85.
20. *Id*. at 885–99.
21. *Id*. at 862–71.
22. *Id*. at 885–88.
23. *Id*. at 894.
24. *Id*. at 860.

materials for credit card fraud.[25] Another comes from the infringing goods space, where sellers, often using quickly seized ephemeral domains, market knock–off designer bags and other cheap–to–produce but high–priced items. In the illegal or infringing goods businesses, a successful enterprise needs a prominent web presence, similar to the mainstream brands. Businesses gain such prominence by having easy–to–recognize domain names and search–optimized sites. The website has to be reasonably well–designed and available to users. One also needs to be able to collect payments from users and to deliver the product to the consumer. Even illicit businesses, such as counterfeit pharmacies, care about reputation because they earn up to thirty–seven percent of their gross revenue from repeat purchases.[26] Thus, customer reviews are important.[27] Turning to botnets, operators face business–like costs too. Cybercriminals have specialization and expertise, as do many other actors in the broader economy, creating a complex market for services.[28] Cybercriminals in these markets must advertise their services, deliver them reliably, collect payment, and (in the case of botnets) maintain a collection of compromised computers. In this last function—botnet maintenance—bot herders, who conscript vulnerable machines into botnets, are in constant conflict with both nation states and sophisticated technology companies. To turn a profit, like ordinary businesses, illegal and infringing good sellers must make many sales.

In both the illegal goods and infringing goods contexts, each critical function to monetizing the crime relies on third party intermediaries. Sellers and marketplaces need domain names, hosting services, access to payment systems, banking services, access to postal or shipping networks, and so on. Many of these intermediaries are probably unaware of misconduct.[29] For various practical reasons, the nature of the web causes

25. Nicolas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*, *in* PROCEEDINGS OF THE 22ND INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 213, 213–24 (2013).

26. Damon McCoy et al., *PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs*, *in* PROCEEDINGS OF THE 21ST USENIX CONFERENCE ON SECURITY SYMPOSIUM 1, 7 (2012), http://cseweb.ucsd.edu/~voelker/pubs/pharmaleaks-usesec12.pdf.

27. BRIAN KREBS, SPAM NATION: THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR 81 (2014).

28. Alvaro A. Cárdenas, Svetlana Radosavac, Jens Grossklags, John Chuang & Chris Hoofnagle, *An Economic Map of Cybercrime,* 2009 TPRC 2–9.

29. Sumayah Alrwais et al., *Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks*, *in* 2017 IEEE

businesses to concentrate their services, making entire enterprises dependent on single intermediaries in some contexts. For instance, Levchenko and collaborators found that just three banks processed transactions for ninety–five percent of the goods advertised by spam in their study.[30] In another study, author Hoofnagle showed that among the most prominent online pharmacies, many shared the same shopping cart and same telephone services for sales.[31] It also appears that the rewards from such activities inure to a small number of actors. For instance, McCoy and colleagues performed an in-depth study of the customers and affiliates associated with three online pharmacy networks.[32] The group observed that affiliate marketers are major purveyors of web spam to promote online pharmacies and that a small number of advertisers in the affiliate network captured the most revenue.[33] In particular, the largest earner of commissions was a company that specialized in web spam, and it made $4.6 million.[34] McCoy and colleagues also found that twenty to forty percent of sales from email spam arise from users who actively open their spam folder and click on links to pharmacy sites.[35]

At the root of this discussion are actors who are perpetrating a wide variety of cybercrimes. These crimes are as diverse as illegally distributing copyrighted content, hacking, and engaging in the trade of illicit goods and services (i.e. drugs, sex trade, human trafficking, etc.). These criminals are exceptionally difficult to pin down because they operate with complex social networks that often span international borders.

SYMPOSIUM ON SECURITY AND PRIVACY 805, 805–06 (2017). "Bulletproof" hosting providers promise to keep users' accounts online even in the face of complaints and legal processes, but users must pay a premium for such guarantees. *Id.* at 805; Krebs, *supra* note 27 at 15.

30. Kirill Levchenko et al., *Click Trajectories: End-to-End Analysis of the Spam Value Chain*, *in* 2011 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 431, 443 (2011).

31. Chris Jay Hoofnagle et al., *Online Pharmacies and Technology Crime*, *in* THE ROUTLEDGE HANDBOOK OF TECHNOLOGY, CRIME AND JUSTICE 146, 155 (M. R. McGuire & Thomas J. Holt eds., 2017).

32. McCoy et al., *supra* note 26.

33. *Id*. at 10–11.

34. *Id*. at 12.

35. Neha Chachra, Damon McCoy, Stefan Savage & Geoffrey M. Voelker, *Empirically Characterizing Domain Abuse and the Revenue Impact of Blacklisting*, *in* 2014 PROCEEDINGS OF THE WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY 1, 5–6 (2014).

The next Sections turn to some of the key actors that depend on or attempt to interfere with intermediaries: botnets, sellers of counterfeit goods, and intellectual property owners.

A. BOTNETS

Botnets are networks of infected computers (the "bots") that are used to conduct illegal operations. In particular, botnets can be used to forward communications (i.e. spam emails, viruses, etc.) to other computers and grow the network, and to execute Distributed Denial of Service (DDoS) attacks that can disrupt all internet use. DDoS attacks were a principal tactic in the first nation–state cyberattacks, thus making botnet mitigation a concern for both businesses and nations.[36]

As targets of legal interventions, botnets are tricky to pin down because of their international and self–propagating nature. Individual bots could be in the homes of consumers all over the world, and could be in the form of the computers and software embedded in internet–connected cameras and even routers.[37] Bots take their direction from remote command and control servers that are generally operated by bot herders. Skilled botnet herders mask these systems, and even distribute control to new domains on predefined schedules. Presumably, the botnet herder knows what new domains will be selected and can compromise them in time to issue new instructions to the bots.[38]

The handoff of the command and control infrastructure offers an opportunity to disrupt botnets—in effect by rustling them from the herder. Technically and legally sophisticated actors such as Microsoft Corporation can use legal processes to seize the domains that the botnet will next connect with. Once seized, a company can issue instructions to the bots to update their software and stop new attacks. For example, a "sinkhole" tactic routes the associated domain names to a new DNS server, which then assigns non–routable addresses to the domains. Basically, this prevents anyone from actually accessing the website where the individual bots receive their instructions, rendering the botnet impotent.[39]

---

36. Steve Mansfield-Devine, *The Growth and Evolution of DDoS*, 10 NETWORK SECURITY 13, 13–14 (2015).

37. Elisa Bertino & Nayeem Islam, *Botnets and Internet of Things Security*, 50 COMPUTER 76, 78 (2017).

38. For a fascinating discussion of these dynamics, see generally MARK BOWDEN, WORM: THE FIRST DIGITAL WORLD WAR (2011).

39. Evan Cooke, Jahanian Farnam, & Danny McPherson, *The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets*, *in* PROCEEDINGS OF THE 2005 STEPS

B. ILLEGAL AND INFRINGING GOODS SELLERS

People intent on selling illegal and infringing goods use their own websites and online marketplaces to do business and point buyers to other internet resources where infringing content may reside. Similarly, they may use social media and other pages to boost infringing services' prominence in search engines.[40]

These actors pose a challenge for law enforcement because it is difficult to discern legal operations from illegal ones. For example, it is difficult to tell whether a handbag sold on eBay is stolen, counterfeited, or simply from a legitimate owner trying to resell an expensive fashion item. In other cases, sellers set up networks of websites that are obviously in the business of knockoffs.

Domain Name Server (DNS) seizure is a common tool leveraged against these easier–to–identify sellers. Because the sellers are typically outside the United States, they are difficult to physically track down, and therefore enforcers have an easier time directly seizing the infringing web domain and other services. The next Section details the prototypical procedure. The basic notion is that the enforcer can take over a domain and prevent anyone from accessing it, therefore shutting down the illegal operations that were being carried out.

C. INTERMEDIARIES AND INTELLECTUAL PROPERTY OWNERS

This Article focuses on intermediaries' capacity to deter and combat cybercrime, and therefore highlights key players, such as technology companies that provide products and act as online platforms, and IP owners that take actions against infringers. These actors are important because when they invest in cybersecurity, they can produce positive externalities for end users and smaller firms.[41] That being said, there are key distinctions between companies involved with combating botnet activity and companies involved with IP enforcement. The former set of actors is intertwined with the governance and security of Internet

TO REDUCING UNWANTED TRAFFIC ON THE INTERNET ON STEPS TO REDUCING UNWANTED TRAFFIC ON THE INTERNET (SRUTI) WORKSHOP 39, 41–42 (2005) ("A bot must communicate with a controller to receive commands or send back information."), https://www.usenix.org/legacy/event/sruti05/tech/full_papers/cooke/cooke.pdf.

40. McCoy et al., *supra* note 26.

41. Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, 140 DAEDALUS 70, 85 (2011); Joel P. Trachtman, *Global Cyberterrorism, Jurisdiction, and International Organization*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 259–63 (Mark F. Grady & Francesco Parisi eds., 2006).

infrastructure, and therefore regularly cooperates with public and private institutions to maintain a secure Internet.[42] The latter set is mainly concerned with preventing the sales of counterfeit, physical goods over online platforms. But in some cases, the two interests mix—as detailed below, botnets are sometimes used to sell counterfeit pharmaceuticals. Although Internet security and IP enforcement are distinct policy areas, they are discussed in tandem because courts employ similar toolkits in approaching both issues.

On the botnet issue, this Article emphasizes Microsoft's role in cybercrime deterrence because of the company's dominance in operating systems and its centrality in cybersecurity. Microsoft's signature product is its Windows operating system, and protecting the integrity of that product is a major goal for the company. Over the course of several years, Microsoft's reputation suffered as various viruses infected machines running Windows, and for some time, almost by definition a botnet was comprised of Windows machines.[43] In 2002, Microsoft announced a major security rethink. It aggressively invested in cybersecurity infrastructure and participated in legal proceedings aimed at taking down the most expansive botnets, thus rehabilitating its product's reputation.[44] Microsoft has gone so far as to use this mechanism—a kind of privately–waged lawfare—against the "Fancy Bear" hacking group suspected to have aided President Trump in his contest against Hillary Clinton.[45] Microsoft's litigation activity is an illuminating example of private activity that leads to more public cybersecurity, because Microsoft's actions arguably had spillover effects for consumers, businesses running Windows machines, and virtually anyone who was impacted by these botnets.

In terms of IP owners, companies that specialize in goods such as fashion products, rather than music and DVD piracy, are more relevant when discussing intermediary–driven approaches to cybercrime.

42. Professor Kristen Eichensehr explains that botnet takedowns are one form of an institutionalized public-private cybersecurity system, where cooperation between dominant technology companies and the government have resulted in remedies for severe security problems. Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 470–72 (2017).

43. *Gates Finally Discovers Security*, WIRED (Jan. 17, 2002, 10:50 AM), www.wired.com/2002/01/gates-finally-discovers-security/.

44. *Id.*

45. Kevin Poulsen, *Putin's Hackers Now Under Attack—From Microsoft*, DAILY BEAST (July 20, 2017, 10:05 PM), https://www.thedailybeast.com/microsoft-pushes-to-take-over-russian-spies-network; Complaint, Microsoft Corp. v. Does, 1:16-CV-993 (E.D. Va. Aug. 3, 2016), 2016 WL 4203923.

Generally, fashion products can either be found in brick–and–mortar stores or through online retailers, and are susceptible to being undercut by knockoffs. This is particularly true for fashion products that trade on exclusive, European labels but are actually made in China rather than Italian or French workshops. The exclusive branding of these products drives high prices, but counterfeits often exhibit identical or good enough indicia of quality. Throughout this Article, companies such as Tiffany, Kate Spade, Gucci, and the like provide examples of enforcers that go after infringers. These retailers face challenges in addressing counterfeit sales, which occur in American markets, such as Amazon and eBay, and non–American markets, such as China's Taobao online marketplace. The ease of creating and distributing counterfeit goods in these domestic and foreign marketplaces invites IP infringement.[46] Furthermore, jurisdictional issues leave American courts with few options to directly deter this sort of activity.

As such, IP owners have developed a toolkit for dealing with counterfeit goods that simply circumvents the CDA 230 regime and its immunities. Enforcers bring lawsuits using Rule 65 of the FRCP to quickly obtain equitable relief. Enforcers also join professional alliances and organizations, cooperate with payment intermediaries,[47] and work directly with online marketplaces to remove infringing products. Because their products are so easily counterfeited, these companies have a strong incentive to invest in lawsuits as well as technological infrastructure that detects and prevents this activity. In turn, consumers presumably benefit from not being duped through online marketplaces. However, for many consumers, cheap knock–offs or higher quality "factory counterfeits" (those created by employees of the authorized factory during a secret, "fourth shift") might be a perfect substitute for the real thing.[48]

46. For instance, companies join organizations like the International Anti-Counterfeiting Coalition (IACC) in response to widespread counterfeiting. *See History & Mission*, INT'L ANTICOUNTERFEITING COALITION, https://www.iacc.org/about/history-mission (last visited Feb. 2, 2018).

47. Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523, 1548–54 (2015).

48. MM Houck, *Counterfeit Goods*, *in* MATERIALS ANALYSIS IN FORENSIC SCIENCE 449, 449 (Max M. Houck ed., 2016).

IV. JUDICIAL INTERVENTIONS

A. RULE 65 INTERVENTIONS

Whether enforcers are attempting to police intellectual property rights or fight botnets, they rely on obtaining equitable relief through Rule 65. For all practical purposes, as soon as an enforcer obtains a Temporary Restraining Order (TRO), it has legal authority to order intermediaries to deny services to identified suspects and their internet resources. This deterrence by denial approach is intended to block the defendant from enjoying the gains of their alleged cybercrime.

Figure 1: Outline of Legal Steps in Rule 65 Interventions

LEGAL STEP	LEGAL DESCRIPTION	COMMENTS	TIMELINE
Motion for a Temporary Restraining Order	Plaintiff(s) files a motion (often sealed) in District Court requesting a Temporary Restraining Order against one or more Defendants. In the motion, the Plaintiff lists the trademarks that were infringed upon, the websites involved in the alleged activity, and the requested relief.	At this stage, the Plaintiff demonstrates harm, reasons why injunctive relief is necessary, and lists the domain names they would like to seize, along with exhibits with screenshots of offending sites. The TRO is sought without notice to the defendant.	Preparation for this action presumably takes some time because of the need to document infringements and domain owners.

LEGAL STEP	LEGAL DESCRIPTION	COMMENTS	TIMELINE
Court issues Temporary Restraining Order	Court issues the TRO. The TRO typically includes a Temporary Injunction, a Temporary Transfer of the Defendant Domain Names, and a Temporary Asset Restraint, among others. At this point, the Plaintiff has achieved the most important legal intervention to deny the benefits of cybercrime to the suspect.	Not only does the Order enjoin the Defendants from further infringement, it also extends to intermediaries that are served with it. For instance, domain name registries are required to either change the infringing pages' registrar or make them inactive and untransferable, and registrars must transfer Defendants' domain names to a registrar account of the Plaintiff's choosing.	Approximately 1 week. Under Rule 65, TROs are to be *temporary*, thus courts assign short durations to them and prioritize a follow-up hearing for preliminary injunction.
Preliminary Injunction	Court restrains Defendants from operating their allegedly infringing websites	Interventions from the TRO stage are sustained until trial. However, in practice, enforcers typically obtain a default judgment.	4 weeks

LEGAL STEP	LEGAL DESCRIPTION	COMMENTS	TIMELINE
Summons served	Clerk of the Court issues summons to Defendants. If Electronic Service is granted, e-mail and posting notice on websites serves as sufficient notice	Defendants are put on notice to respond to claims	Within days of granting of preliminary injunction
Motion to Enter Default Judgment/Final Judgment Order	Finalizes the actions undertaken with the TRO and Preliminary Injunction	At this stage, intermediaries are directed to ensure that the Plaintiff gets permanent control over the infringing domain names	Approximately 2 weeks

A TRO is an extraordinary measure because it can be obtained entirely *ex parte*. The plaintiff bears the burden to show "specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition" and the plaintiff must both certify its efforts to give notice to the adverse party and explain why notice should not be required.[49] The purposes of this remedy are to preserve the status quo and prevent irreparable harm until a hearing can take place.

As explained below, once an enforcer obtains a TRO, it has a powerful remedy to use against intermediaries. The court order commands top–level

49. FED. R. CIV. P. 65.

domain name systems to replace the names of the infringing authoritative name servers with a new name controlled by the plaintiff. In some cases, IP enforcers operate the newly acquired domain and notify the public that illegal goods were once sold on it.[50] In botnet cases, enforcers can use the TRO to direct the domain into a sinkhole, which prevents anyone from accessing it.[51] Thus, the intermediary, in cooperation with the Registry, routes the names to the sinkhole, then prevents anyone from accessing the names once they have been successfully placed there.

Rule 65 interventions can occur with incredible speed, relative to ordinary litigation in the notoriously overburdened federal court system. Figure 1 gives an overview of the basic steps and timeline that parties can expect in an expeditious Rule 65 intervention. Plaintiffs enjoys a statutory privilege to get a hearing and relief quickly, often with key documents filed under seal. In the next Section, this Article gives context to these steps in a trademark infringement case.

A TRO is not necessarily a "silver bullet" and it can have some negative repercussions. When cybercriminals are attacked through their intermediaries, the intervention can cause fragmentation—a turn to smaller intermediaries, where substitutes are available. In the case of botnets, operators might move their command and control systems to DNS provided by a bulletproof host, switch to a peer–to–peer architecture, or cloak more of their systems using Tor or I2P. Also, the intervention may be overbroad, negatively affecting innocent third parties.[52]

All judicial interventions are also subject to claimant abuse—situations where one invokes the procedures in order to engage in censorship or anticompetitive behavior. Such abuse comes about both intentionally and unintentionally. Yet, Rule 65 interventions have two checks built into them that are not present in private–sector remedial schemes (discussed in Part VI below). First, Rule 65 requires that movants file a security bond to pay the costs and damages of any party "wrongfully enjoined or

50. Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322, 2016 WL 8577031 (N.D. Ill. Aug. 25, 2016).

51. United States v. John Doe 1, No. 3:11-CV-00561 (D. Conn. Apr. 13, 2011), ECF. No. 32.

52. In forthcoming work, cybersecurity experts Sasha Romanosky and Zachary K. Goldman propose a framework for defining the scope and severity of "collateral damage" in the cyber realm. Sasha Romanosky & Zachary K. Goldman, *What Is Cyber Collateral Damage? And Why Does It Matter?*, LAWFARE BLOG (Nov. 15, 2016, 1:30 PM), https://www.lawfareblog.com/what-cyber-collateral-damage-and-why-does-it-matter.

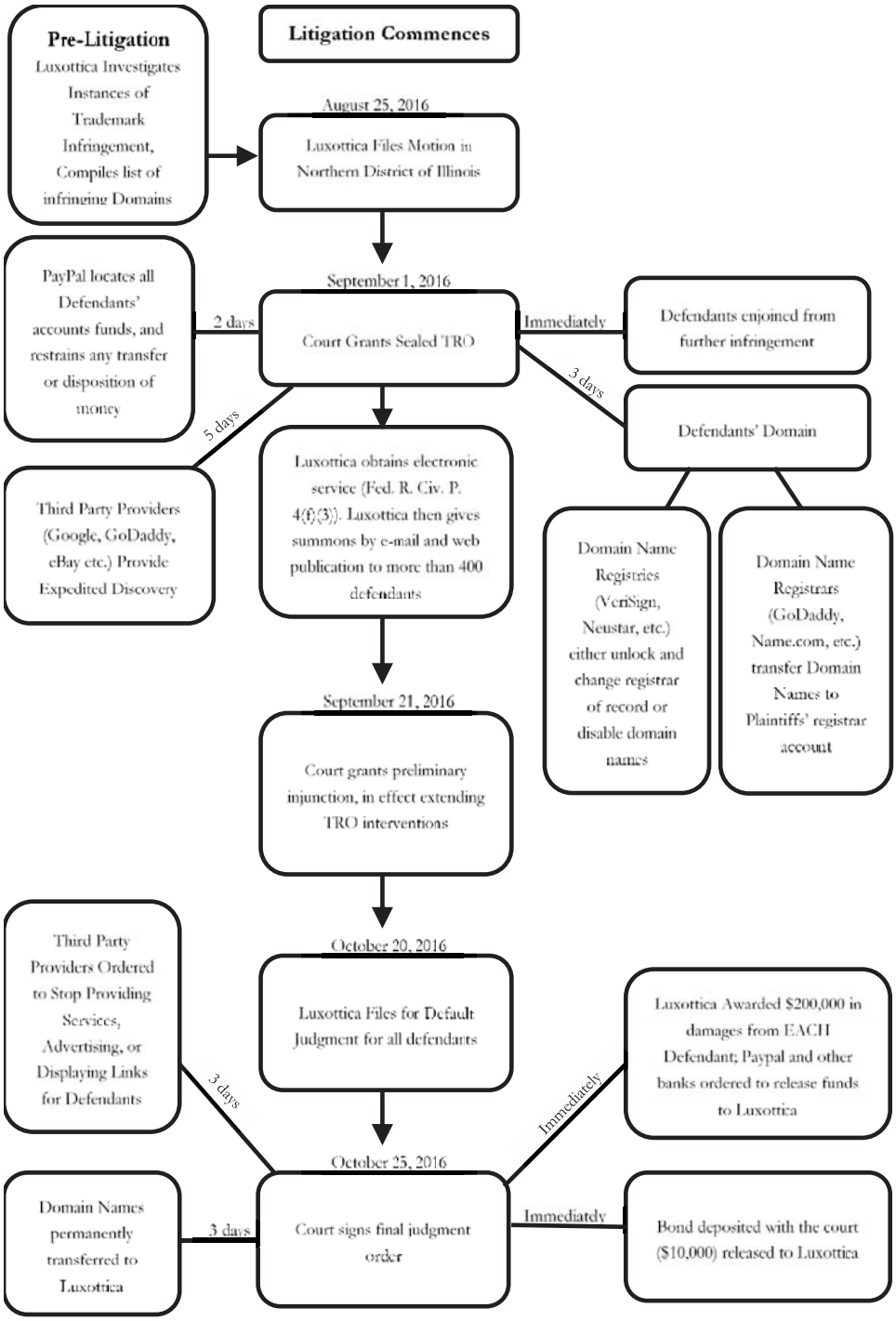
restrained."[53] Notice of this bond is provided to intermediaries served with the court's order. Second, the intervention is court supervised. Thus, lawyers, as officers of the court, will presumably avoid abusive applications of TROs and preliminary injunctions lest they attract negative judicial attention.

1. Examples from Trademark Infringement

In Figure 2, we visualize the typical case flow for a Rule 65 intervention. We chose the *Luxottica* case as it illustrates several of the most notable features of this intervention, namely the rapid pace from the filing of the lawsuit to the final order, and the massive scope given to the IP enforcer for seizing and controlling assets, coopting intermediaries into compliance, and recovering damages.

53. FED. R. CIV. P. 65(C).

Figure 2: Illustration of TRO Procedure with Luxottica Case



Luxottica, a company that owns many sought–after brands of eyewear, provides a paradigmatic example of employing Rule 65 in the IP enforcement context, one that is troubling in scale and presages a kind of automation of litigation. As outlined in Figure 2, in a single 2016 case, Luxottica sued 478 defendants that were allegedly infringing marks in operating 1,024 domains and 52 marketplaces (most of which were "stores" on eBay).[54] The case caption is so long that it occupies five pages in print, and in the electronic filing system, the defendants are listed as "The Partnerships and Unincorporated Associations Identified on Schedule A." Luxottica filed the case on August 24, 2016, and received a TRO nine days later against all the defendants.[55] Luxottica argued that relief without notice was necessary because the targeted domain owners would likely move their operations if told that an enforcement action was afoot. The lack of notice gave Luxottica another advantage—Rule 65 requires that TROs lacking notice receive a hearing as soon as possible, and so Luxottica received a preliminary injunction less than a month from the date the complaint was filed.

Figure 2 outlines the basic steps taken by Luxottica to obtain the TRO and the many varied entities bound by it. Luxottica filed a required form with the PTO to indicate it was about to enforce its trademark. It obtained a $10,000 bond filed with the court per Rule 65.[56] That amount was proposed by Luxottica and approved by the court, but presumably could have been raised or lowered to prevent abuses raised by the facts of the case. Luxottica prepared the motions for equitable relief, and in the process, filed straightforward exhibits, thousands of pages long, with screenshots of websites clearly showing Luxottica's product trademarks. But it did not engage in test purchases, which are required to identify the merchant processing account(s) used by a website to accept credit card payments. Its proof that the targeted websites were infringing was based on an in–house investigator's deductive reasoning: the websites were not

54. Amended Complaint, Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322 (N.D. Ill. Aug. 25, 2016), 2016 WL 8577031.

55. Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322 (N.D. Ill. Sept. 1, 2016), ECF No. 30 (granting temporary restraining order in a minute entry).

56. Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322 (N.D. Ill. Sept. 7, 2016), ECF No. 31 (reflecting posted bond of $10,000).

in Luxottica's approved channel list, the suspect websites had lower prices, and the websites offered shipping to the United States.[57]

Luxottica moved for and obtained approval to give adverse parties electronic notice. It gave notice via email and by posting a notice of the lawsuit on the very web properties it seized with the TRO. But none of the defendants answered the summons within twenty–one days. Thus, just two months after filing the complaint, Luxottica had a final, default judgement in the case—for $200,000 per defendant (in theory, up to $95 million).[58]

Luxottica's relief is also typical of cases in the field,[59] and this relief is broad. The Luxottica court found the defaulting defendants liable for willful trademark infringement and counterfeiting, false designation of origin, cybersquatting, and for violating a state consumer protection law. The final judgment gave Luxottica permanent transfer of the 1,024 domains, and seizure of the defendants' PayPal accounts. It also ordered broad categories of unnamed businesses not to service the defendants when they were displaying Luxottica's marks. Luxottica's order covered marketplaces (such as eBay and Alibaba), web hosts, sponsored search engine and ad–word providers, credit cards, banks, merchant account providers, third party processors, payment processing service providers, search engines, and domain name registrars. These are all the intermediaries critical to operating a web business.

2. Examples from Hacking and DDoS

TROs are also the legal tool of choice for public and private enforcement against botnets.[60] Botnets are notoriously difficult to police

57. Amended Complaint, Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations Identified on Schedule "A," No. 1:16-cv-08322 (N.D. Ill. Aug. 25, 2016), 2016 WL 8577031.

58. *Id.*

59. We found no cases with the number of defendants in Luxottica, but others follow a similar procedure and have even shorter times to relief. For instance, in one case, a plaintiff received a TRO in one day. *See* Kate Spade, LLC v. Zhou, No. 1:14-cv-05665 (S.D.N.Y. Aug 28, 2014), ECF 9 (granting TRO in a minute order). We cannot assess the frequency of these suits but they appear to be quite common. A search in Bloomberg Law's Dockets search for civil suits where Chanel was a plaintiff and the keywords "trademark infringement" and "domain" were present returned 163 results. The cases date back to 2001 and were initiated in federal courts all over the country. Twenty–six of the cases were "open" as of May 3, 2017.

60. Eichensehr, *supra* note 42, at 470–72. Not covered here are the extraordinary nonlegal efforts private–sector technology companies take to neutralize botnets. One well–documented example comes from the campaign to fight Conficker. *See* BOWDEN, *supra* note 38, at 94–96.

with traditional deterrence by punishment because botnet herders are likely to operate outside the United States.[61] Although botnets are a different security concern, the TRO procedure is remarkably similar to the IP context illustrated earlier. The landscape includes public and private sector collaboration, and the use of civil and criminal mechanisms to obtain information and to seize assets. The basic sequence of events is that either the U.S. government or a sophisticated technology company such as Microsoft files for a TRO in District Court, the TRO is granted under seal, the command–and–control servers are either physically or remotely seized, and finally Microsoft issues a software update that commands infected bots to disengage from the network and cease malicious behavior. The following Sections highlight the use of TROs in the Coreflood, Rustock, and Kelihos cases to illustrate the efficacy and issues to consider.

a) The Coreflood Botnet

Coreflood was a Russian–based botnet that infected computers across the public sector, as well as other critical systems belonging to hospitals, businesses, etc. At its peak, it infected over two million machines, and it could repurpose these computers for several different tasks—to attack other computers with denial–of–service attacks, to provide an anonymous platform for hackers for multi-stage attacks, and to capture user keystrokes, thereby enabling the botnet controllers to discover credit card numbers and bank login information.[62] The privacy and security implications of Coreflood and other botnets are profound, making those infected vulnerable to many different kinds of wrongs.

The government averred that a single Coreflood command server "held approximately 190 gigabytes (GB) of data, recorded from 413,710 infected computers while unsuspecting computer users were browsing the Internet."[63] The government claimed that Coreflood was used to steal six–figure sums from a number of small businesses, even ones that had used two–factor authentication to carefully protect banking accounts.[64]

61. In 2009, the Federal Trade Commission, using its powers to obtain injunctions for unfair and deceptive trade practices, took down 3fn, which was regarded as among the last US-based "bulletproof" hosts. Fed. Trade Comm'n v. Pricewert LLC, No. C-09-2407 RMW, 2010 WL 2105614, at *1 (N.D. Cal. Apr. 8, 2010).

62. United States v. John Doe 1, No. 3:11-CV-00561 (D. Conn. Apr. 13, 2011), ECF No. 32.

63. *Id.* at 32

64. *Id.*

In a civil complaint, the government obtained a TRO from a district court, along with several search warrants in different districts. The TRO sought by the Justice Department authorized the Internet Systems Consortium (ISC), a nonprofit, to swap out privately owned command–and–control servers and turn them over to the government.[65] Once this happened, Microsoft released a patch through its Malicious Software Removal Tool, which instructed machines infected with Coreflood to remove the program.[66]

In requesting the TRO in the civil case, the government argued that obtaining a search warrant was impracticable, explaining that botnet situations justified use of the special needs exception to the general preference that the government obtain a warrant for a search or seizure. The government assured the court that it would not collect any protected information or communications from the computers infected with Coreflood. The court granted the TRO but prohibited the agencies from storing, reviewing, or using information unrelated to the data needed to battle the botnet.[67] Interestingly, although the government obtained the TRO through a civil procedure, the Department of Justice also announced that it would pursue a criminal prosecution.[68] The line between civil and criminal procedure blurs as TROs are used as tools to combat criminal activity, which is why this case reflects the basic due process concerns at play when the government, intermediaries, and nonprofits cooperate on operations that implicate constitutional and statutory interests.

b) The Rustock Botnet

Rustock was a self–propagating botnet that was responsible for a large portion of spam emails worldwide. This botnet used a Trojan virus to infect machines that received spam communications, and was difficult to detect. Several previous attempts to bring down Rustock failed due to its ability to quickly restore its capacity after any partial attack.[69]

---

65. *Id.*

66. Press Release, U.S. Dep't of Justice, Department of Justice Takes Action to Disable International Botnet (Apr. 13, 2011), https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

67. United States v. John Doe 1, No. 3:11-CV-00561 (D. Conn. Apr. 13, 2011), ECF No. 51.

68. Press Release*, supra* note 66

69. MICROSOFT CORP., BATTLING THE RUSTOCK BOTNET: SECURITY INTELLIGENCE REPORT 7 (2011), https://lammgl.files.wordpress.com/2011/03/battling-the-rustock-threat_english.pdf ("Rustock checks for the presence of kernel debuggers . . . and . . . also tries

Microsoft, in cooperation with Pfizer (which suffered potential reputational and financial harm because Rustock sent spam emails for knock–off Viagra), the U.S. government, and the University of Washington, finally disabled the botnet through Operation b107.[70] Microsoft brought suit in the Western District of Washington, and obtained a TRO that authorized the implementation of the operation under seal.[71] Accompanied by U.S. Marshals, Microsoft seized equipment used in Rustock, performed forensic analysis on it, and concluded that the evidence pointed to a Russian–based operation.[72]

Microsoft gained standing to pursue this action under a combination of the CAN-SPAM Act and the Lanham Trademark Act, in part because Microsoft's trademarks are used to propagate malware.[73] Pfizer's involvement was key for invoking the Lanham Act, and for triggering a sense of urgency—the drugs sold via Rustock were passed off as real, but in test purchases, some proved to differ from those sourced from Pfizer's supply chain.[74] Moreover, Microsoft ensured that the court order was under seal until the operation was complete, so as to avoid tipping off the botnet herders in advance. As in the Coreflood proceedings, the plaintiffs justified their actions by noting that Microsoft would respect due process concerns and that this intervention was the narrowest possible.[75] It also filed a $170,000 bond. Microsoft updated the court weeks after it seized IP

to maintain code integrity by constantly checking itself for modifications using CRC32 checksums, and by scanning itself for software breakpoints (0xCC).").

70. *Id.* at 3.

71. Complaint, Microsoft Corp. v. John Does 1-11 Controlling a Computer Botnet Thereby Injuring Microsoft and Its Customers, No. 2:11-cv-00222 (W.D. Wash. Mar. 1, 2011), 2011 WL 921612.

72. Peter Bright, *How Operation b107 Decapitated the Rustock Botnet*, ARS TECHNICA (Mar. 22, 2011), https://arstechnica.com/information-technology/2011/03/how-operation-b107-decapitated-the-rustock-botnet/.

73. Microsoft Corporation's Application for an Emergency Temporary Restraining Order, Seizure Order, and Order to Show Cause Re Preliminary Injunction, Microsoft Corp. v. John Does 1-11 Controlling a Computer Botnet Thereby Injuring Microsoft and Its Customers, No. 2:11-cv-00222 (W.D. Wash. Feb. 9, 2011), 2011 WL 1193746.

74. *Id.* ("Counterfeiters deceive patients into believing that the products they offer are safe and effective medicines from trusted pharmaceutical companies such as Pfizer, upon whose integrity they have relied to receive medicines that permit them to live happier and healthier lives.").

75. Bright, *supra* note 72.

addresses and domain names to report that it had received no requests to reinstate these resources.[76]

c) The Kelihos Botnet

One ongoing example of government and intermediary efforts to thwart a botnet is the Kelihos case.[77] Kelihos is a botnet that functions in a similar fashion to Rustock by using spam to infect peer computers with malware.[78] In this case, the program is able to conduct a range of operations including DDoS attacks and stealing cryptocurrency wallets.[79] On April 10, 2017, the Justice Department announced that it was undertaking actions to dismantle the botnet.[80] Unlike in the Coreflood case however, the government invoked the 2016 Amendments to Rule 41 of the Federal Rules of Criminal Procedure (FRCrP), instead of Rule 65 of the FRCP.[81] Under the new language, the federal government is able to seek a warrant to search a computer that is hidden through the use of technology (such as anonymizing software like Tor or I2P), and sue in just one jurisdiction in cases where devices in five or more districts are implicated (as opposed to all districts).[82] This is an important step because previously the government struggled to remotely search anonymized criminals, and faced high litigation costs arising from the requirement to sue in multiple districts.[83]

As indicated earlier, the government generally used a combination of TROs from civil procedure and criminal investigations to cooperate with intermediaries in botnet cases. In this case, the government relied solely on criminal procedure. However, despite using the FRCrP instead of the FRCP, the technical procedure used looks to be the same as previous

76. Microsoft Corporation's Status Report Re Preliminary Injunction at 2, Microsoft Corp. v. John Does 1-11 Controlling a Computer Botnet Thereby Injuring Microsoft and Its Customers, No. 2:11-cv-00222 (W.D. Wash. Apr. 4, 2011), ECF No. 43.

77. Press Release, U.S. Dep't. of Justice, Justice Department Announces Actions to Dismantle Kelihos Botnet (Apr. 10, 2017), https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0.

78. *Kelihos*, N.J. CYBERSECURITY & COMMC'S. INTEGRATION CELL (Dec. 28, 2016), https://www.cyber.nj.gov/threat-profiles/botnet-variants/kelihos.

79. *Id*.

80. Press Release, *supra* note 77.

81. FED. R. CRIM. P. 41(B)(6)(B).

82. *Id*.; FED. R. CIV. P. 65.

83. Press Release, *supra* note 77; Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, U.S. DEP'T JUST. (June 20, 2016), www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

botnet cases. The government got authorization to take control of command–and–control servers, identified IP addresses, and then turned them over to an intermediary to sever connections between the botnet herder and the servers. As in the previous cases, Microsoft used its software updates to instruct infected computers to delete the virus that propagated the botnet. This case may signal a legal framework that courts will use going forward, but it substantially represents the same combination of the government cooperating with an intermediary to seize servers and dismantle them via a sealed court order.

3. Criticisms of Rule 65 Interventions

Despite the apparent efficacy of Rule 65 TRO interventions in both trademark and botnet applications, this tool is criticized for potential overbreadth. As demonstrated in *Luxottica*, federal courts, notorious for their slow processes, place these cases at the top of the docket. Because the invocation of Rule 65 expedites litigation, it is possible to get powerful, broad remedies in a matter of days or weeks. Electronic service further greases the wheels by eliminating the labor–intensive but salient event of being physically served with process. These court orders are also usually heard *ex parte*, and the restraining order is granted under seal to avoid alerting infringers and perpetrators.

In the IP context, the orders are broad in that they cover a wide variety of actors. The TRO allowed Luxottica to compel action from hundreds of defendants, domain name registrars, payment processors, search engines, online marketplaces, and advertisers. Not only did the TRO reach a massive number of actors (many of which were intermediaries), it compelled action from them within a matter of days. This breadth reflects that judicial harmony with enforcers that pursue infringers alone is inadequate, and therefore courts lean on intermediaries to undertake actions to punish and prevent unlawful behavior.

Annemarie Bridy mounts a strenuous critique of domain seizure in *Three Notice Failures in Copyright Law*.[84] Bridy argues that seizure without notice to domain owners infringes both First and Fifth amendment rights.[85] Her argument is at its strongest when enforcers seize domains with significant non–infringing purposes, such as file sharing systems. Non–infringing uses may not be apparent to courts, and enforcers may see

84. Annemarie Bridy, *Three Notice Failures in Copyright Law*, 96 B.U. L. REV. 777 (2016).

85. *Id.* at 802–14.

these services as primarily piracy operations. Enforcers tend to target niche players, and as Bridy explains, innocent users of such systems are presumed guilty.[86]

The botnet context suffers from similar concerns, with the additional problem of creating collateral damage for innocent third parties. For instance, Microsoft requested a TRO to sink several computers that were generating dynamic IP addresses to conduct illegal activities. The TRO was directed at NO-IP.com, but inadvertently took down many sites that were using dynamic IP addresses for legitimate purposes.[87] Users, as well as organizations like the Electronic Frontier Foundation, criticized this action.[88] Again, the controversy stemmed from the sudden nature of the action because the TRO was carried out *ex parte* and under seal. Moreover, Microsoft was criticized for its outsized role in seeking and implementing the legal and technical actions necessary for the TRO. In virtually every case examined, Microsoft, in partnership with the federal government and other companies, was responsible for developing and implementing the software that disrupted botnets. Microsoft's role here is natural for the obvious reason of Microsoft's product being a dominant operating system worldwide, and indeed this is an attractive feature in terms of effectively combating large and diffuse botnets. However, this also means that Microsoft is disproportionately powerful, and can cause unintended harms by pursuing an overbroad TRO. Without any way to raise concerns before implementation, potential victims must rely on Microsoft's and a court's foresight of potential harms to innocent parties.

More generally, there is continued discussion about the extent to which preliminary injunctions may properly conscript intermediaries. Rule 65 orders can only bind certain entities, including parties, entities related to the parties (such as their servants, employees, and agents), and those in "active concert or participation" with the parties.[89] What is the status of

86. *Id.* at 806–07 (discussing the case of Megaupload users).

87. Brief in Support of Application of Microsoft Corporation for an Emergency Temporary Restraining Order and Order to Show Cause Regarding Preliminary Injunction, Microsoft Corp. v. Mutairi, No. 2:14-cv-00987 (D. Nev. Jun 19, 2014); *see also* Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237 (2014).

88. *See generally* Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 SANTA CLARA HIGH TECH. L.J. 163 (2014); Lerner, *supra* note 87, at 250–60; Robert McMillan, *How Microsoft Appointed Itself Sheriff of the Internet*, WIRED (Oct.16, 2014), https://www.wired.com/2014/10/microsoft-pinkerton/.

89. FED. R. CIV. P. 65(D)(2)(C).

payment providers or domain registrars in these cases? Courts do not specify their precise role in orders. For example, in one case, CloudFlare, which provides reverse–proxy service, complied with a preliminary injunction that required it to terminate user accounts that used specific domain names.[90] CloudFlare, however, opposed obligations to filter on a continuing basis for customers using the domain name "grooveshark."[91] In this effort, CloudFlare found an ally in the Electronic Frontier Foundation (EFF), which argued that this preliminary injunction required CloudFlare to act as "enforcers" of the plaintiff's trademark and could potentially affect customers who were not using the domain name in an infringing matter.[92]

This situation contains many parallels to other cases examined here. As noted, the final judgment order in the *Luxottica* case compelled search engines and online marketplaces to stop serving the defendants, implying an obligation to continue monitoring their systems for infringing behavior.[93] Like with the CloudFlare example, this puts intermediaries in the position of continually enforcing another party's IP rights. While this arrangement is pragmatic, since the fact that infringers will not realistically comply with court orders means that focusing on intermediaries is more effective, intermediaries may challenge overreliance on their capacity and willingness to pursue infringers on behalf of IP owners.

Internet commerce has a different logic than offline business operations. Firms supplying infringing content probably never meet any of the third–party service providers that make their operation possible. Some of the intermediary services may be offered free, or at a very small cost. Additionally, the various intermediaries probably are neither aware of nor wish to be involved with infringement. For these and other reasons, Bridy recommends that enforcers should prove that "nonparty service providers . . . either expressly or tacitly agreed to act in furtherance of a common

90. Arista Records, LLC v. Tkach, 122 F. Supp. 3d 32, 34 (S.D.N.Y. 2015) .

91. *Id*. at 35.

92. Mitch Stoltz, *Victory for CloudFlare Against SOPA-like Court Order: Internet Service Doesn't Have to Police Music Labels' Trademark*, ELECTRONIC FRONTIER FOUND. (July 15, 2015), https://www.eff.org/deeplinks/2015/07/victory-cloudflare-against-sopa-court-order-internet-service-doesnt-have-police.

93. Luxottica Grp. S.p.A. v. Zhou Zhi Wei, No. 17-CV-05691, 2017 WL 6994587, at *3 (N.D. Ill. Sept. 12, 2017)

plan of infringement."[94] Such a burden of proof would render Rule 65 interventions toothless.

V. GOVERNMENT–LED INTERVENTIONS

This Part details two ways in which the government uses the courts and administrative powers to police intellectual property and computer hacking crimes. The first section covers seizures of websites using the Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act.

A. PRO-IP ACT DOMAIN SEIZURES

Government and intellectual property owners have used domain name seizures to interdict websites that host, or even simply link to, illegal content. Domain names identify things connected to the Internet, and link them to IP addresses. Domain names are considered a core component of Internet governance, and are a fundamental part of establishing property rights on the Internet.

Special legal authority for domain name seizure comes from the PRO-IP Act, which gave birth to interagency efforts to interdict online IP violations.[95] Basically, the federal government seizes a website accused of engaging in illegal activity, making it impossible to reach it by searching its alphanumeric name. It is still generally possible to reach it by directly entering its numeric IP address. Most consumers probably will never figure this out, so the blocked sites are, in effect, boarded up. Once seized, the government can continue its investigation of the website's alleged infringement, before pursuing further legal action.[96]

DNS seizures are useful because they are effective at targeting internet resources complicit in illegal behavior. For these one–off instances, DNS seizures are easy to undertake, and only require cooperation between the government and domain name registrars. Moreover, they can be used to pursue websites whose owners may be difficult to track down or may live outside the United States, without requiring a lengthy legal proceeding.

---

94. Bridy, *supra* note 84, at 831.

95. Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. 110-403, 122 Stat. 4256.

96. Kopel, *supra* note 18, 863–67; Dave Piscitello, *Guidance for Preparing Domain Name Orders, Seizures & Takedowns*, ICANN (Mar. 7, 2012), www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf.

Yet, DNS seizures are controversial because of the potential overbreadth and potential lack of regard for process. They can be overbroad in that the government can identify targets for seizure that are not directly related to illegal activity. Relatedly, it can bring down the websites without the defendants showing up in court. Without strong procedural protections, the government can seize domain names that are not actually associated with illegal activity.[97]

For instance, the Rojadirecta and Dajaz1 cases reflected this flaw in PRO-IP Act DNS seizures. Rojadirecta was a website that linked to other websites illegally streaming sportscasts, and Dajaz1 was a website that offered hip-hop commentary and reviews, as well as song samples. Rojadirecta's legality was upheld in Spanish courts two years prior to the U.S. seizure.[98] In both cases, the government seized the domain names, but the owners of the websites successfully challenged the orders and regained control of the web properties.[99] In the Dajaz1 case, the U.S. government never came up with the adequate evidence to justify a permanent injunction, and thus handed the domain back to its original owner.[100] In both cases, the domain owners were deprived of the properties for over a year. For even the most successful web businesses, a short service outage can be ruinous.[101]

DNS seizures are criticized for the same reason that civil forfeiture has become widely scrutinized: they take control of property whose owners lack the means to challenge the government's allegations. As was the case with TROs, the Rojadirecta and Dajaz1 cases were heard *ex parte* and were seized without notifying the owners beforehand. The owners of these domains successfully challenged their seizure, but the vast majority of the more than 1,000 domains seized never challenge the government.[102] The breadth and muscularity of intellectual property rights obviously raises the specter of these mechanisms being used for censorship.

---

97. *See* Bridy, *supra* note 11, at 1378 (showing illustrative problems in the areas of copyright and child pornography enforcement).

98. Jennifer Martinez, *US Government Dismisses Piracy Case Against Rojadirecta Site*, HILL (Aug. 29, 2012, 9:26 PM), http://thehill.com/policy/technology/246529-us-government-dismisses-case-against-rojadirecta.

99. Kopel, *supra* note 18, at 880–81.

100. David Kravets, *Feds Seized Hip-Hop Site for a Year, Waiting for Proof of Infringement*, WIRED (May 3, 2012, 5:00 PM), https://www.wired.com/2012/05/weak-evidence-seizure/.

101. Puerto 80 Projects, S.L.U. v. United States, No. 11-3983 (S.D.N.Y June 20, 2011).

102. Kopel, *supra* note 18, at 860.

B. GOVERNMENT INTERVENTION IN FINANCIAL SERVICES INTERMEDIARIES

Aside from court–authorized actions, the U.S. government also uses administrative power to investigate and disrupt cybercrime. Multiple agencies claim jurisdiction over cybercrime because it implicates financial security, protection of critical infrastructure, criminal statutes, and intellectual property protections. As such, both the Justice Department and the Treasury Department launched financial security programs that touch on cybercrime.

Operation Choke Point was a President Obama-era Justice Department program that focused on banks and their business clients.[103] Specifically, it targeted certain merchant categories that were recognized as being high–risk. For instance, it covered money laundering, consumer exploitation (scams, payday lenders, etc.), and online gambling. Essentially, the program aimed at uncovering information about exploitative and illegal practices by leveraging banks' access to unique insights about the merchants that banks connect to the payments system.[104] The Justice Department, focused on payment providers, targeted banks with subpoenas and investigative attention to determine whether they were aware of or were colluding in fraud perpetrated by partner payment providers.[105] This investigatory attention caused banks to sever relationships with both questionable and lawful merchants, raising the ire of the business community and triggering Congressional blowback.[106] The Trump administration ended operation Choke Point in 2017.[107]

---

103. Jessica Silver-Greenberg, *Justice Department Inquiry Takes Aim at Banks' Business With Payday Lenders*, N.Y. TIMES (Jan. 26, 2014) https://dealbook.nytimes.com/2014/01/26/justice-dept-inquiry-takes-aim-at-banks-business-with-payday-lenders/.

104. *Id.*

105. U.S. HOUSE OF REPRESENTATIVES COMM. ON OVERSIGHT & GOV'T REFORM, THE DEPARTMENT OF JUSTICE'S "OPERATION CHOKE POINT": ILLEGALLY CHOKING OFF LEGITIMATE BUSINESSES? (2014), https://oversight.house.gov/wp-content/uploads/2014/05/Staff-Report-Operation-Choke-Point1.pdf.

106. *Id.*

107. Letter from Stephen F. Boyd, Assistant Att'y Gen., Dep't of Justice, to the Honorable Bob Goodlatte, Chair, Comm. on the Judiciary, U.S. House of Representatives (Aug. 16, 2017), http://alliedprogress.org/wp-content/uploads/2017/08/2017-8-16-Operation-Chokepoint-Goodlatte.pdf.

Other examples include President Obama's Executive Order (EO) 13694,[108] which was amended by EO 13757.[109] In EO 13694, the U.S. Department of Treasury was authorized to place a block on all property and property interests in the United States that are associated with cybercrime by placing individuals and entities on the specifically designated nationals and blocked persons list (SDN).[110] This intervention is similar to other Treasury holds placed in response to illegal activities,[111] and its authority stems from the International Emergency Economic Powers Act.[112] With this authority, the Treasury, in conjunction with the Justice Department can freeze bank accounts, deplete them, and generally prevent their owners from accessing them. As of this writing, the government has not placed anyone on the 13694 list.

EO 13757, adopted late in President Obama's tenure, amended the earlier order in light of Russian state–sponsored attacks on American presidential candidates Hillary Clinton and Senator Marco Rubio.[113] EO 13757 specified that activities "interfering with or undermining election processes or institutions" trigger designation on the SDN.[114] Over forty individuals and entities have been placed on the SDN under the EO 13757 process.[115]

These programs are useful in that they can target cybercriminals who are not physically located in the United States. In both cases, the government leverages the fact that financial institutions are central to cybercriminal operations. Because much cybercrime is financially

108. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, 80 FED. REG. 18,077 (Apr. 1, 2015).

109. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 82 FED. REG. 1 (Dec. 28, 2016).

110. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, 80 FED. REG. 18,077 (Apr. 1, 2015).

111. *See* Transnational Criminal Organizations Sanctions Regulations, 31 C.F.R. § 590 (2017) (using the 2016 classification of PacNet as a significant transnational criminal organization pursuant to E.O. 13581 as an example of SDN interventions against intermediaries for online crime); *see also Specifically Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, U.S. DEP'T OF TREASURY (Feb. 2, 2018), https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx [hereinafter *Dep't of Treasury SDN*].

112. 50 U.S.C. § 1701 (2012).

113. *Dep't of Treasure SDN*, *supra* note 111.

114. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 82 FED. REG. 1 (Dec. 28, 2016).

115. *Id.*

motivated, identifying and dismantling perpetrators' financial assets is a key tool for deterring it.

Financial interventions are also more likely to effectively disrupt cybercriminal activity than DNS seizures. Since there are many registrars, DNS seizures may only temporarily take infringing websites offline. A study by Wang and collaborators found that domain name seizures did not significantly reduce the number of counterfeit online stores found in search engine results for luxury goods.[116]

There is evidence suggesting that DNS seizures are not a one–time intervention, and companies must bring a series of lawsuits to continue pursuing infringers, which may help explain why they do not significantly reduce the number of counterfeit stores in the long–run. Indeed, in the *Luxottica* cases, the court order also instructed PayPal to restrain payment accounts based in China and Hong Kong, indicating that simply seizing the domain names in question was not an adequate remedy.[117]

VI. PRIVATE REMEDIATION PROCEDURES

Under pressure from intellectual property owners, some market platforms have developed their own takedown policies. Large platforms allow for their users to report IP infringement, and then take actions to remove the infringing listings or transactions. These interventions do not require the explicit consent of law enforcement, and rather reflect the intermediaries' effort to mitigate the harm done by cybercriminals. The following Section details some examples of these mechanisms, and then discusses the general advantages and disadvantages of self–regulation.[118]

116. David Y. Wang, Matthew Der, Mohammad Karami, Lawrence Saul, Damon McCoy, Stefan Savage & Geoffrey M. Voelker, *Search + Seizure: The Effectiveness of Interventions on SEO Campaigns*, *in* PROCEEDINGS OF THE 2014 CONFERENCE ON INTERNET MEASUREMENT CONFERENCE 359 (2014).

117. Luxottica Grp. S.p.A. v. Zhou Zhi Wei, No. 17-CV-05691, 2017 WL 6994587, at *3 (N.D. Ill. Sept. 12, 2017).

118. The survey here includes efforts focused on large platforms that control a huge transaction space, such as eBay and the Visa payment network. However, the literature includes discussions of countless other private remediation programs. For instance, Liu et al. explore policy changes that affect domain name acquisition in the .cn ccTLD and the effects of a verification service that screened domains for illegal pharmacy activities. He (Lonnie) Liu et al., *On the Effects of Registrar-Level Intervention*, *in* PROCEEDINGS OF THE 4TH USENIX WORKSHOP ON LARGE-SCALE EXPLOITS AND EMERGENT THREATS (2011).

A. EBAY VERO PROGRAM

eBay's Verified Rights Online (VeRO) Program is geared towards helping IP owners prevent sellers from illegally marketing merchandise, unauthorized copies, and other branded materials. The process largely relies on IP owners reporting infractions to eBay, but provides participants with a few different options for large–scale and chronic infringements. This program provides a concrete example of how an online marketplace takes actions against infringers. eBay is a particularly good example because virtually all of the products it sells are supplied by users, therefore breaking the channel controls that some luxury brands use to maintain vertical price fixing and exclusivity. It is thus important to understand that brand owners may be objecting to any sale of their branded merchandise in addition to items that are infringing or counterfeit.

The procedure for VeRO is straightforward and easily accessible. Anyone (including people and companies that do not have listings on eBay) who owns a product or piece of intellectual property is eligible to participate. An interested party must sign up for a VeRO account and provide links to the infringing products. Then, the user emails "vero@ebay.com" to notify eBay that s/he would like to assert IP rights. Finally, the party submits a "Notice of Claimed Infringement (NOCI)" form.[119]

This process is geared toward individual violations, but naturally some parties may have larger needs. eBay provides for users to search for IP infringement through manual monitoring, setting up a "Watch List," or hiring a full–time monitoring agency. eBay imposes no fee for reporting infringement or for creating watch lists, but companies incur expenses in employee time or in hiring boutique monitoring services.[120]

B. VISA IP ENFORCEMENT

Visa, like MasterCard, is a payment network, an ISP–like entity for banks and merchants that exchange money in order to process consumer

119. *Notice of Claim Infringement*, EBAY http://pics.ebay.com/aw/pics/pdf/us/help/community/NOCI1.pdf (last visited Feb. 2, 2018).

120. General information about the program is available on eBay's website. *See Verified Rights Owner Program*, EBAY, http://pages.ebay.com/seller-center/listing/create-effective-listings/vero-program.html (last visited Feb. 2, 2018). A list of participating members is also available. *See VeRO Participant Profiles*, EBAY, http://pages.ebay.com/seller-center/listing/create-effective-listings/vero-program.html#m17-1-tb3 (last visited Feb. 2, 2018).

purchases. Visa thus can monitor aspects of transactions but it cannot track the specific items purchased by the consumer.[121] However, Visa can monitor suspicious merchants and link their activity across different banks.

Visa voluntarily searches for potential IP infringement in its payment systems, and attempts to enforce IP owners' rights.[122] Visa has at least two different procedures that it uses for its IP takedown activities, one of which is an online form that victims can fill out identifying a merchant who has infringed on IP. The website claims that individuals may file five claims per month, and afterward Visa investigates each claim and arbitrates.[123]

More detailed information comes from a 2011 congressional testimony by Visa on the issue of IP takedowns. Visa explained that it deals with complaints directly via emails to "Inquiries@visa.com."[124] One important note is that Visa and other credit card companies do not generally have direct relationships with individual merchants who accept their cards as payment.[125] Instead, merchants have relationships with payment companies that link them to the network. After receiving a complaint, Visa does a test transaction to identify the payment company that signed up the suspected infringing merchant.[126] Visa then instructs the payment company to investigate the merchant, and report within five business days.[127] After reviewing the report, Visa has the payment company send a "comply or terminate" notice to the suspected infringer.[128]

121. Chris Jay Hoofnagle, Jennifer M. Urban & Su Li, *Mobile Payments: Consumer Benefits & New Privacy Concerns* (Berkeley Ctr. for Law & Tech., Research Paper 2012), https://ssrn.com/abstract=2045580.

122. *Targeting Websites Dedicated to Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 1 (2011) (statement of Denise Yee, Visa, Inc.), https://www.judiciary.senate.gov/imo/media/doc/11-2-16%20Yee%20Testimony.pdf.

123. *Report Intellectual Property Abuse*, VISA, https://usa.visa.com/Forms/report-ip-abuse-form.html (last visited Feb. 2, 2018).

124. *See* Yee, *supra* note 122, at 12.

125. *Id.* at 6.

126. *Id.* at 12–13.

127. *Id.*

128. *Id.*

C. INTERNATIONAL ANTICOUNTERFEITING COALITION (IACC)

The IACC is a nonprofit that brings together various actors concerned with international IP infringement.[129] The organization is composed of over 250 member organizations, including private businesses, law firms, security firms, and government organizations.[130] It also hosts semiannual conferences dedicated to informing members about best practices, and coordinate efforts to clamp down on IP infringement.[131]

The IACC offers a suite of services to its members, namely the "RogueBlock" and "MarketSafe" features. RogueBlock is a back–end network that connects IP owners to investigators, payment companies, the government, and related actors.[132] When infringement occurs, the IACC processes reports and distributes them to the relevant intermediaries on behalf of its members.[133]

MarketSafe is a direct partnership between the IACC and Alibaba to take down counterfeiting infringers on the online marketplace, Taobao.[134] It includes access to "expedited take–down procedures" that presumably guarantee members a quick turnaround on their reports of IP infringement on the website.[135] Essentially, the IACC provides investigative and administrative services to its members by specializing in searching for infringement, producing relevant evidence, and filing the proper documentation in IP takedown cases.[136]

D. BACKPAGE.COM: PRIVATE REMEDIATION AS A SCAFFOLD FOR CRIMINAL PROSECUTION

Backpage.com is a popular online classified ads site, similar to Craigslist. But Backpage is known for its adult escort ads, which are believed among the not–born–yesterday to be a front for organizing online

129. For an in–depth discussion, see Annemarie Bridy, *supra* note 47, at 1548–54.
130. INT'L ANTICOUNTERFEITING COALITION, supra note 46.
131. *Id.*
132. *IACC RogueBlock®*, INT'L ANTICOUNTERFEITING COAL., http://www.iacc.org/online-initiatives/rogueblock (last visited Feb. 2, 2018).
133. *Id.*
134. *IACC MarketSafe®*, INT'L ANTICOUNTERFEITING COAL., http://www.iacc.org/online-initiatives/marketsafe (last visited Feb. 2, 2018).
135. *Id.*
136. *Id.*

prostitution and child sex trafficking.[137] Experts in human trafficking believe that Backpage does not simply provide a substitute for offline child sex markets, but rather contributes to an explosive growth in reports of child sex trafficking: astonishingly, the National Center for Missing and Exploited Children claims that 73% of the child sex trafficking reports it receives involve Backpage.[138]

Years ago, law enforcement agencies pressured credit card networks to stop accepting payments initiated on Backpage.[139] By July 2015, American Express, Visa, and MasterCard all agreed to stop such payments.[140] In a December 2016 criminal complaint, the State of California charged Backpage's operators with money laundering and conspiracy for creating fake e-commerce sites to evade American Express' payment ban.[141] The state alleges that the defendants instructed escorts and pimps on how to buy "credits" on these third party sites that were actually destined for Backpage's escort business.[142]

The State charged the Backpage operators with financial crimes because an earlier attempt to prosecute them ended in failure—a state court judge held that under CDA 230, the operators we not liable for the classified ads posted by third parties.[143] The State brought the new charges just weeks after the failed prosecution.[144]

---

137. S. COMM. ON HOMELAND SEC. & GOV'T AFFAIRS, BACKPAGE.COM'S KNOWING FACILITATION OF ONLINE SEX TRAFFICKING 1 (2017) [hereinafter REPORT ON BACKPAGE.COM].

138. *Id.*

139. Rebecca Hersher, *Backpage Shuts Down Adult Ads in the U.S., Citing Government Pressure*, NPR (Jan. 10, 2017, 11:23 AM), https://www.npr.org/sections/thetwo-way/2017/01/10/509127110/backpage-shuts-down-adult-ads-citing-government-pressure.

140. Michelle Hackman, *Backpage Files Suit Against Cook County Sheriff Over Credit Card Service*, WALL ST. J. (July 21, 2015, 2:35 PM), https://www.wsj.com/articles/backpage-files-suit-against-cook-county-sheriff-over-credit-card-service-1437496670.

141. Criminal Complaint, People v. Ferrer, No. 16FE019224 (Cal. Super. Ct. Sept. 20, 2016), 2016 WL 6091120. American Express differs from MasterCard and Visa in that it is a "closed-loop" system, and as such, it operates as a network, processor, and merchant acquirer. This direct relationship with merchants may explain why the California Department of Justice focused on Backpage.com's alleged evasions with respect to American Express and not open-loop systems.

142. *Id.*

143. Trial Order, People v. Ferrer, No. 16FE019224 (Cal. Super. Ct. Nov. 16, 2016), 2016 WL 6905743.

144. Felony Criminal Complaint, People v. Ferrer, No. 16FE024013 (Cal. Super. Ct. Dec. 23, 2016), 2016 WL 7884408.

E. COMMENTS ON VOLUNTARY AND SELF–REGULATING PROCEDURES

Voluntary procedures avoid use of the courts, thereby avoiding costs and delays. Moreover, they allow for the victims of infringement and fraud to directly deal with the infringement. These are important advantages because they avoid the costs associated with lawsuits, and encourage victims to take advantage of these policies. Because of these features, these platforms establish credibility in their services. As seen in the Backpage.com example, voluntary procedures can also lay the groundwork for government enforcement actions.

On the other hand, the lack of transparency obscures actual practices and subtle shifts in policy. Self–regulatory procedures hide the actual penalties levied by intermediaries on various actors. They also make it possible for the intermediary to weaken its posture over time, perhaps by reducing penalties once scrutiny from enforcers eases. Self–regulatory procedures can hide awful practices that indicate the most noxious uses of the platform—for instance, Backpage.com was filtering terms that indicated child sex trafficking such as "Amber Alert."[145] Finally, a lack of transparency obscures how self–regulatory systems distribute seized proceeds from suspected cybercrime.

Another major disadvantage to these approaches is that they all rely on self–reporting from the victim. Although eBay and Visa allow for some automation in their services, they are not inherently designed to deal with large–scale fraud or theft. By default, they are designed to deal with individual complaints, which means they are probably more effective at isolated incidents involving smaller victims.

This feature makes voluntary efforts difficult to rely on when dealing with botnets, large crime networks, and systemic fraud. Although organizations like the IACC attempt to clean up marketplaces like Taobao, self–regulation on its own does not necessarily alleviate the structural problems with these platforms. Perhaps this is why some enforcers have pursued litigation or administrative enforcement actions.

VII. SUMMARY AND CONCLUSION

Cybercrime is often presented as an intractable problem because it can be committed by users under a cloak of anonymity and committed from jurisdictions without effective rule of law. Intermediaries are presented as

145. REPORT ON BACKPAGE.COM, *supra* note 137.

being broadly shielded from liability for their users' actions. This Article explains that these frames obscure the reality of deterring financially–motivated cybercrime: such cybercrime shares characteristics of ordinary businesses. Like ordinary businesses, financially–motivated cybercrime is an activity of scale, not a jackpot activity such as robbing a bank. Criminals need to optimize their processes, make sales, and critically, they rely on many different intermediaries for everything from marketing, to web hosting, to delivery of products. Reliance on intermediary service providers gives enforcers the opportunity to disrupt these networks. While CDA 230 provides intermediaries great cover for demands to take down some material, anti–botnet and IP enforcers have found some success using FRCP Rule 65 to compel intermediaries to hand over or block resources used by cybercrime networks, typically within days of filing suit.

Intermediaries are in a tussle among law enforcement, powerful brands, legitimate users, and rogue users. Enforcers have found effective technical fixes (sinkholes, delisting a website's alphanumeric name, etc.), yet there is no one simple solution that works across all classes of crime.

Narrower gateways offer more powerful interventions. For instance, a prior study by author McCoy and collaborators found that payment platforms, because of their breadth and oligopoly status, have more power over cybercriminals than interventions in the DNS.[146] There is more competition in domain name administration, and far too many top–level–domains (e.g. .com, .net, and so on) to control the entire space.[147]

Moreover, these types of interventions can cause serious collateral damage that disrupt legitimate operations or otherwise impose costs on legitimate users. Considering that these interventions require intensive cooperation among the government, nonprofits, and corporate actors, the motivations of these actors must be balanced as to not interfere with other public policy goals like fair market competition, strong privacy protections, and encouragement of innovation.

It is unlikely that enforcement approaches focused on intermediaries will cause decentralization and turns to harder–to–disrupt technologies, such as cryptocurrencies. This is because financially–motivated

146. Damon McCoy, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M. Voelker & Stefan Savage, *Priceless: The Role of Payments in Abuse-advertised Goods*, *in* PROCEEDINGS OF THE 2012 ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 845, 845–46 (2012)

147. He Liu et al., *supra* note 118.

cybercriminals need to appeal to a mass consumer population. For these consumers, PayPal and similarly–mainstream payment mechanisms are accessible, whereas decentralized ones are difficult to use and generally go unused by ordinary consumers.[148] For instance, author McCoy and colleagues found that blocking DDoS–for–hire services from PayPal caused an almost immediate, short term reduction in availability of such services. The McCoy team observed that a DDoS service that only accepted cryptocurrency Bitcoin had a two percent conversion to paid subscriber rate, while two competitors that accepted PayPal had fifteen percent and twenty–three percent conversion rates, respectively.[149] At least for financially–motivated criminal enterprises that depend on sales to average consumers—the purchasers of online pharmaceuticals and counterfeit handbags discussed in this Article—profitmaking will depend on low transaction costs and simple access procedures for consumers. Skeptics may invoke the technically–shrouded, sophisticated marketplace Silk Road as a counternarrative, but Silk Road was small in comparison to the enormity of the international drug trade and there is some evidence that it served a business–to–business function for drug dealers.[150] Presumably drug dealers finding a supply for drugs to resell would be more motivated to learn the intricacies of cryptocurrencies, but many ordinary consumers cannot.

Enforcers will likely continue their focus on intermediaries to police their brands and to break up botnets. These efforts raise concerns over due process, property rights, and privacy rights. This Article shows that IP enforcers are able to take control over thousands of domain names, including those that include goods other than the infringing items. Interventions are often done *ex parte*, and may not require notice to the affected websites under Rule 65. In fact, attacks on botnets must omit this notice for fear that cybercriminals can avoid the attempts to sinkhole the

148. Paul Vigna, *People Love Talking About Bitcoin More Than Using It*, WALL ST. J. (Apr. 12, 2017, 5:30 AM), https://www.wsj.com/articles/people-love-talking-about-bitcoin-more-than-using-it-1491989403.

149. Mohammad Karami, Youngsam Park & Damon McCoy, *Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services*, *in* PROCEEDINGS OF THE 25TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 1033 (2016).

150. Judith Aldridge & David Décary-Hétu, Not an 'Ebay for Drugs': The Cryptomarket "Silk Road" As a Paradigm Shifting Criminal Innovation (May 13, 2014) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643.

botnet. It is important that interventions reflect appropriate humility in light of the lack of adversarial process.

PLATFORM LAW AND THE BRAND ENTERPRISE

Sonia K. Katyal[†] *& Leah Chan Grinvald*[††]

ABSTRACT

The emergence of platforms has transformed the digital economy, reshaping and recasting online transactions within the service industry. This transformation, as many have argued, has created new and unimagined challenges for policymakers and regulators, as well as for traditional, offline companies. Most scholarship examining platforms discuss their impact on employment law or consumer protection. Yet trademark law, which is central to the success of the platform enterprise, has been mostly overlooked within these discussions. To address this gap, this article discusses the emergence of two central forms of platform entrepreneurship—the platform, or "macrobrand" and the platform service provider, or the "microbrand." As we argue, the macrobrand and microbrand interact with trademark law–and one another–in ways that challenge conventional models of trademark application and expose their existing limitations. In exposing how platform architecture causes an unsustainable tension between these two formations, this Article suggests a two-prong approach utilizing both legislative adjustments to trademark law, as well as common law adjustments, to modernize trademark doctrine for the digital economy.

DOI: https://doi.org/10.15779/Z38GM81P1M

† Chancellor's Professor of Law; Co-Director, Berkeley Center for Law and Technology, University of California, Berkeley.

†† Associate Dean for Academic Affairs and Professor of Law, Suffolk University Law School. We would like to thank the following for helpful feedback and conversation: Frederick Mostert, Michael Birnhack, Assaf Jacobs, Christopher Hoofnagle, Andrew Bridges, Aaron Rubin, Brianna Schofield, Jennifer Urban, Jim Dempsey, and the organizers of the Platform Law Symposium. We would also like to thank Andrea Hall and Amy Egerton-Wiley for excellent research assistance. We welcome feedback at either skatyal@berkeley.edu or lgrinvald@suffolk.edu.

TABLE OF CONTENTS

I. INTRODUCTION

If Web 1.0 was about access to information via the Internet and Web 2.0 was about the formation of the online marketplace, Web 3.0 is about the platform: the transformation of the offline marketplace, particularly the service industry, by online transactions.[1] The application of algorithmic tools to the economies of leisure, consumption, services, and manufacturing has produced a profound transformation of the service economy.[2] Even more, the movement of many of these services to cloud providers has an even greater, transnational character. This move facilitates the development of a global infrastructure; as two commentators observe, the emergence of platform and cloud architecture "reconfigure

1. Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 94 (2016).

2. *See generally* Martin Kenney & John Zysman. *The Rise of the Platform Economy*, 32 ISSUES IN SCI. & TECH. 61 (2016) (citing work by Stuart Feldman, Kenji Kushida, Jonathan Murray, and others discussing this transformation).

globalization itself."[3]

At the same time, the definitional and regulatory complexities that accompany the emergence of platforms have posed some significant challenges for lawyers and commentators. At its simplest, a platform "points to a set of online digital arrangements whose algorithms serve to organize and structure economic and social activity."[4] This not only produces – and is facilitated by – a system of shared tools, technologies and interfaces enabling decentralized innovation, but also creates a hybrid blend of market and social interactions that we have not yet seen before in the digital economy.[5]

Yet in order to explore the legal complexities that platforms create, we must also analyze some of the differences between them. Platforms can be characterized by the particular services that they offer or the business models that they disrupt.[6] Some of these platforms, like Google and Facebook, offer communication tools, social media, and information; others, like Etsy, eBay, and Amazon operate as online marketplaces; while still others provide infrastructure and tools to build more platforms, like Amazon Web Services.[7] One could characterize platforms based on labor-market arrangements, like crowdsourcing (Amazon Mechanical Turk, as an example) and on-demand services (Uber, TaskRabbit and others).[8] Some platforms facilitate entrepreneurship, and others have more hierarchical arrangements that rely on contractor-like arrangements.[9]

As Orly Lobel and others have explained, while the label of a "platform" is intentionally broad, it represents a myriad of new business models that disrupt previous economies of production, consumption, finance, knowledge and education, among other elements.[10] If traditional

---

3. *Id.* at 61.

4. *Id.* at 65. For more on the definition and attributes of platforms, see Diane Coyle, *Making the Most of Platforms: a Policy Research Agenda*, (The Jean-Jacques Laffont Digital Chair, Working Paper), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2857188.

5. *See* Kenney & Zysman, *supra* note 2 at 67.

6. *See* ARUN SUNDARAJAN, THE SHARING ECONOMY: THE END OF EMPLOYMENT AND THE RISE OF CROWD-BASED CAPITALISM 77 (2016).

7. Kenney & Zysman, *supra* note 2, at 61.

8. Ruth Berins Collier et al., The Regulation of Labor Platforms: The Politics of the Uber Economy 7 (Mar. 2017) (unpublished manuscript), http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Reg-of-Labor-Platforms.pdf.

9. Sundarajan, *supra* note 6, at 77-79.

10. *See* Lobel, *supra* note 1, at 98–99.

categories of business relied on the consistency of dyads like employer/employee, seller/buyer, and producer/consumer, platform entrepreneurship exploits networks where these lines become blurred through sharing and pooling economies.[11] By lowering transaction costs through connecting consumers directly with producers, platform economies promise less waste, and a greater ability to break both supply and demand into what Lobel describes as discrete, modular units – short term housing assistance and help with minor tasks such as furniture installation, cooking, driving, and the like.[12] "Web 3.0," Lobel argues, "is transforming the lifestyle of the masses, not only better matching a static equilibrium of supply and demand, but also generating different sets of supply and demand and reconfiguring markets."[13]

The benefits of a platform economy are manifold. The trend toward modularity (which Yochai Benkler describes as "granularity") transforms ordinary exchanges into opportunities for market-based capitalism, reducing barriers to entry, increasing dynamism and precision in pricing and services.[14] Platforms can reduce overall prices for consumers because of the lowered transaction and overhead costs they are associated with by connecting consumers with producers more directly and in real-time.[15] They enable entities to take advantage of underutilized assets, like space, and provide access to services that may have previously been unavailable.[16] They can improve the consumer experience by offering new services that others have failed to offer.[17] Finally, they can utilize systems to track ratings and reputation, thereby ensuring trust between the consumer and the service provider.[18] Collectively, platforms also underscore a significant shift from theories of ownership and property; the "consumption culture" that we inhabit becomes replaced with a focus on access instead.[19] "Owning a car," Lobel writes, "is not as important as the ability to use one when needed."[20]

---

11. *Id.* at 100–01.

12. *Id.* at 109–10.

13. *Id.* at 114.

14. *Id.* at 109.

15. Rudy Telles Jr., *Digital Matching Firms: A New Definition in the 'Sharing Economy' Space*, U.S. DEP'T OF COMM. ECONOMICS AND STATISTICS ADMIN., at 11.

16. *Id.* at 13.

17. *Id.* at 14.

18. *Id.*

19. Lobel, *supra* note 1, at 110.

20. *Id.* at 110.

Yet these new economies usher in complex questions of both definition and regulation. Within this spectrum of views, some have expressed fear that the platform economy facilitates the avoidance of welfare-enhancing laws like long-term employment contracts, insurance, and quality control regulations.[21] As Lobel argues,

> Proponents romantically envision the platform as a return to the days free from corporate dominance, when interactions happened directly and intimately between individuals, when design was bottom-up and relationships were based on community rather than markets. For opponents, it is a dystopian uber-capitalist development in which every interaction becomes the basis of market exchanges, privacy and leisure are lost, and Silicon Valley style-libertarians become richer at the expense of everyone else.[22]

Central to these questions remains the ubiquity of the brand enterprise, which affects nearly every layer of platform architecture. Trademarks are central to the success of the platform economy, but few commentators have really delved into the question of how trademark law both governs – and is governed by – the emergence of these new economies. Thus, this Article lays out a spectrum of trademark interactivity, identifying the emergence of two central forms of platform entrepreneurship, and then analyzes how the design and architecture of these new forms ushers in new challenges and opportunities for the modernization of trademark law altogether.

Trademark law plays a central, determinative role in the success or failure of the platform enterprise. At the broadest level, in Part II, this Article argues that the platform economy facilitates the emergence of what is called "macrobrands" – the rise of platform economies whose sole source of capital inheres in the value of the brand itself – the Airbnbs, Ubers, and eBays of the world.[23] At the narrowest level, Part III argues

21. *Id.* at 130–37. *See also* Nathan Heller, *Is the Gig Economy Working?*, NEW YORKER, May 15, 2017, https://www.newyorker.com/magazine/2017/05/15/is-the-gig-economy-working; Collier et al., *supra* note 8.

22. Lobel, *supra* note 1, at 105.

23. Others, too, have used the macro and micro brand terminology to describe similar patterns of user engagement and marketing, albeit in a non-platform context. *See, e.g.,* JOSE MARTI ET AL., *Brand Engagement*, *in* THE ROUTLEDGE COMPANION TO THE FUTURE OF MARKETING 253 (Luiz Moutinho et al. eds., 2014) (discussing the role of each structure in reaching consumers); T. Scott Gross, MICROBRANDING: BUILD A

that the platform economy, with its empowerment of the individual, has also facilitated a parallel emergence of the "microbrand" – the rise of discrete, small enterprises made up of individual businesses, each of whom have a strong interest in utilizing the basic principles of branding and trademark protection.

Indeed, this Article views the platform economy as a central opportunity to modernize existing trademark law to accord with the challenges of these new business models. As shown in Part II and Part III, the interaction between macrobrands and microbrands challenges trademark law to evolve to address the new issues presented by platform economies. At the same time, however, our existing frameworks are capacious enough to meet the challenges platforms pose, underscoring the wisdom of the basic, bedrock trademark principles in the process. In Part IV, we outline a host of suggestions to modernize, rather than displace, trademark law for the digital economy. While change can occur by legislation or voluntary measures, this Article focuses specifically on the formation of statutory safe harbors and the modification of the standards for infringement in common law. As this Article shows, these changes can both protect and encourage the vibrancy of the platform economy in an age of legal uncertainty.

II. PLATFORM ARCHITECTURE AND THE RISE OF THE MACROBRAND

As Julie Cohen has argued, the emergence of the platform economy is deeply intertwined with the rise of informational capitalism.[24] Digital platforms have resulted from the intersection of three recent economic developments: the first involving the propertization of intangible resources, the second involving the dematerialization of industrial production, and the third involving the integration of systems of barter and exchange within information platforms.[25] As she observes, platforms do not "enter" or "expand" markets; instead, they replace them by

POWERFUL PERSONAL BRAND & BEAT YOUR COMPETITION (2002) (discussing ways to build a personal or local brand).

24. Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 132, 135 (framing the rise of informational capitalism that parallels the rise of industrial capitalism) [hereinafter Cohen, *Platform Economy*]; *see also* JULIE E. COHEN, *Between Truth and Power*, *in* INFORMATION, FREEDOM AND PROPERTY THE PHILOSOPHY OF LAW MEETS THE PHILOSOPHY OF TECHNOLOGY 57 (Mireille Hildebrandt & Bibi van den Berg eds., 2016).

25. Cohen, Platform Economy, *supra* note 24 at 132.

rematerializing them with new forms of transactional possibility.[26]

Economists have referred to some platforms as "multi-sided platforms" where two or more sides engage in commercial transactions, such as Airbnb, eBay, Uber, Xbox, etc.[27] Many of these companies utilize a model where independent contractors, rather than hired employees, deliver requested services to the client.[28] Further, multi-sided platforms can be characterized by two additional elements: (1) "they enable direct interactions between two or more distinct sides," each of whom retain some control over the key terms of the transaction, such as the terms and conditions of the purchase; and (2) "each side is affiliated with the [existing] platform," meaning that both sides make platform-specific investments that enable them to communicate directly with one another.[29] Take, for example, Airbnb. Instead of directly providing short-term lodging to its customers, Airbnb facilitates transactions between those seeking such lodging, and those offering the lodging. The parties offering the lodging are not employees of Airbnb, but they are affiliated with Airbnb as "hosts." The parties seeking the lodging are also affiliated with Airbnb as "guests."

Today, platforms like Uber and Airbnb, while remaining part and parcel of the sharing economy, also retain a significant degree of control over their hosting activities.[30] Indeed, some commentators have argued that these platforms rest on an arbitrage between the regulation of established businesses, which are held to regulatory standards regarding the treatment of workers, consumers, customers, and markets, and the comparably greyer areas of platform regulation in addressing these entities.[31] "In the current manifestation," commentators argue, "the platform operator has unprecedented control over the compensation for and organization of work, while still claiming to be only an intermediary."[32] Because of the regulatory absence in these arenas, platforms have been able to gain an unprecedented degree of power, a

26. *Id.*; *See also* Tarleton Gillespie, *The Politics of Platforms*, 12 NEW MEDIA & SOC'Y 347 (2010) (further discussion of platforms); Nick Srnicek, PLATFORM CAPITALISM (2017).

27. Andrei Hagiu & Julian Wright, *Multi-sided platforms*, 34 INT'L J. OF INDUS. ORG. 162, 162 (2015).

28. *Id.*

29. *Id.* at 163.

30. Kenney & Zysman, *supra* note 2, at 62.

31. *Id.*

32. *Id.*

power that some have argued may be even more formidable than early factories in the Industrial Revolution.[33] The absence of regulatory reach, coupled with the nimble path of innovation in the platform economy, has a profound effect on the reorganization of society, markets, and firms; as some have observed, "[w]hatever we call the transformation, the consequences are dramatic."[34]

Network effects are central to the success of the platform enterprise, because they demonstrate that the more users subscribe to a platform, the more that platform increases in value.[35] As a product increases in popularity, it increases in dominance, risking the increase in barriers to entry for external entities.[36] An additional network effect is also created by "learning-by-doing," leading users to prefer using the same platform because of its success in both learning the consumer's preferences, and from the consumer's own preferences in relying on the same tool of information.[37] As more and more users are drawn to the platform, it increases in its efficiency, because it is more able to process requests efficiently based on the success of its algorithms in using – and acquiring– -larger and larger quantities of data.[38]

While these effects are often positive for the everyday user, they may also be detrimental from the perspective of other market entrants. This is because platforms can take on gatekeeping functions that can exclude forms of competition, like blocking offerings from outside sellers, or by recommending only applications and sites that exist within its ecosystem.[39] As a result, platforms can exclude others from markets by regulating what is and is not available, thereby distorting the reality of what the marketplace offers to the consumer.[40]

While much ink has been spilled in analyzing and discussing the

33. *See id*.

34. *Id*.

35. Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH. L.J. 1239, at 1244, n.26 (forthcoming 2017) (quoting Margrethe Vestager, *How competition supports innovation*, speech at Regulation4Innovation conference, at https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/how-competition-supports-innovation_en (May 24, 2016)).

36. *Id.* at 7.

37. *Id.* at 7–8.

38. *Id.* at 8.

39. *Id.* at 18.

40. *Id.* at 22.

overall effect of platform arrangements on the labor economy and civil rights protections, fewer pieces have addressed the central role of trademark law in the platform enterprise. Yet trademark and branding practices are implicated within nearly every element of platform architecture and entrepreneurship, raising central questions for the role of regulation. Consider an example. Parking Panda is a platform that enables users to find and secure parking spots.[41] The term "Parking Panda" itself functions as both a trademark and a brand (we will explain the difference between the two below).[42] Yet given its existence as part of the platform ecosystem, Parking Panda itself does not own the garages or the parking spaces it advertises on its platform; rather, these are owned mainly by individual parking companies. These companies have their own trademarks, such as "Icon Parking" or "ABM Parking Services," two large parking companies based in New York City.[43]

In the platform enterprise, trademarks function just like other trademarks in the sense that they serve informational and economic functions.[44] By enabling consumers to trust that their experience of a certain product can be consistently associated with a particular trademark, trademarks lower consumer search costs.[45] Yet trademarks play an even more central role in platform entrepreneurship because they enable consumers to identify clusters of marks with a particular platform, thereby facilitating the reduction of transaction costs that are essential to a platform's success. For example, with the Parking Panda platform, both sets of marks, the Parking Panda's and the parking companies', inform consumers that their parking experience will be similar to their previous experiences, thereby enabling purchasers to rely on their previous

41. *See* PARKING PANDA, *How It Works,* https://www.parkingpanda.com/how-it-works (last visited Jun. 29, 2017) (allowing advance parking reservation from computers or in real-time from mobile phones).

42. U.S. TRADEMARK NO. 4295552 (registered mark for "Parking Panda," operating an online marketplace that allows drivers to find and rent parking spaces and users to rent out their parking spaces."); *See* PARKING PANDA, *The Year of Parking Panda A 2016 Edition,* https://www.parkingpanda.com/year-in-review (last visited Jun. 29, 2017).

43. *See* PARKING PANDA, *Search for Parking in New York City* (last visited Jun. 29, 2017) (images on file with authors).

44. William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 J.L. & ECON. 265, 369 (1987) (A trademark conveys information that allows the consumer to say to himself, "I need not investigate the attributes of the brand I am about to purchase because the trademark is a shorthand way of telling me that the attributes are the same as that of the brand I enjoyed earlier.").

45. *Id.*

decisions.

Branding, too, is an essential aspect of this enterprise.[46] Brands, on one hand, incorporate a business's trademark, but instead of being primarily informational in nature, they also convey an *experience* to the consumer. Particularly in a platform ecosystem, brands tell the consumer about the other individuals who buy the product, thereby creating a community of likeminded purchasers.[47] For example, although Parking Panda aims to help users "find and reserve parking," the company describes its mission as much more than just parking assistance:

> "[t]hrough Parking Panda, drivers plan and commute smarter by booking guaranteed parking in advance. Parking Panda customers are empowered with the ability to search and compare thousands of parking options and prices in more than 40 cities throughout North America."[48]

Through this statement, Parking Panda attempts to create a community of "smart commuters,"[49] a consumer identity and experience, which is their "brand," while also having their related trademark, "Parking Panda."

---

46. *See* Deven R. Desai, From Trademarks to Brands, 64 FLA. L. REV. 981, 985 (2012) ("The corporate dimension of branding creates a strategic asset that allows a corporation to forge not only a product symbol, but also a connection with consumers so that consumers look beyond price when they make a purchasing decision."); Sonia K. Katyal, *Trademark Cosmopolitanism*, 47 U.C. DAVIS L. REV. 875, 890 (2014) ("the trademark represents both a global visual receptacle and a vehicle for all of the emotive and personality characteristics that advertisers hope to associate with a particular brand."); Irina D. Manta, *Branded*, 69 SMU L. REV. 713, 734 (2016) ("Brands, and trademarks as part of them, lead consumers to purchase products that have been designed and marketed to invoke experiences and feelings in the minds of the consumers that influence what products they buy and how they experience the products. Consumers send messages about themselves through the medium of trademarks and seek social status through the same.").

47. *See* Katya Assaf, *Brand Fetishism*, 43 CONN. L. REV. 83, 95 (2010) (discussing the consumer communities of brands such as Apple, Saab, Bronco, and Harley-Davidson); Deborah R. Gerhardt, *Social Media Amplify Consumer Investment in Trademarks*, 90 N.C. L. REV. 1491, 1495 (2012) ("consumers continue to serve as nodes in the social network, building ties with each other and the brand owner by contributing stories to the brand narrative.").

48. *See* PARKING PANDA, *About Us,* https://www.parkingpanda.com/company (last visited Jun. 29, 2017) (exulting the company's goals in lofty language typically associated with a nonprofit).

49. *Id.*

As this Article has suggested, the "macrobrand" in this example is "Parking Panda," and the "microbrands" comprise the individual parking companies that operate within the Parking Panda ecosystem. Yet the legal protection of trademarks, and by extension, brands, introduces tension into the relationship between macro- and micro-brands. Trademark law encourages owners to provide a consistent level of quality in their products, to ensure consumer confidence and repeat purchases.[50] This is done through granting trademark owners limited exclusivity in their trademarks; for example, only one company can be known as "Parking Panda" for online parking services. In addition, trademark law rewards those owners that are active in policing their marks by granting them "strong" or even "famous" status.[51] Therefore, trademark owners are incentivized to police their marks against not just competitive infringement by others who might "pass off" their goods as those of another producer, but also against related or associative uses.[52] This has led, in some cases, to trademark over-enforcement, particularly in situations where macrobrands receive takedown requests to remove allegedly infringing material that microbrands host on the platform.[53]

Unfortunately, the doctrines governing trademarks and intermediary liability are both confusing and outdated, particularly as applied to platforms. This next subsection shows how this standard has played out in both the real space and online context to demonstrate the particular complexities platforms face. Special attention, too, is placed on alternative standards of contributory liability, specifically emerging from Europe and Canada, which have taken different approaches. Finally, we compare the existing approach in trademark law with that taken in the copyright context, which will lay the foundation for suggestions to reform existing law.

A. CONTRIBUTORY LIABILITY: *INWOOD* AND BEYOND

The dominant test of contributory liability in the platform economy is derived from the Supreme Court case of *Inwood Laboratories v. Ives Laboratories*.[54] This case addressed the question of whether manufacturers of generic drugs should be held liable for pharmacies that packaged and

50. *See* Jordan Teague, *Promoting Trademark's Ends and Means through Online Contributory Liability*, 14 VAND. J. ENT. & TECH. L. 461, 465 (2012).

51. *Id.*

52. *Id.*

53. *Id.* at 476.

54. Inwood Labs. v. Ives Labs., 456 U.S. 844 (1982).

sold drugs under infringing packaging labels.[55] The Supreme Court held that a manufacturer and/or distributor could only be held liable for contributory infringement if it could be shown that they "intentionally induce[d] another to infringe a trademark, or if it continue[d] to supply its product to one whom it knows or has reason to know is engaging in trademark infringement . . . ."[56] Later cases have refined this standard to provide that a defendant who takes a "willfully blind" approach (meaning that an actor "suspect wrongdoing and deliberately fail to investigate") can rise to the level of contributory infringement.[57] But both elements – suspicion and failure to investigate – need to be present, because courts have held that simply failing to take precautions to limit counterfeiting, for example, does not qualify as "willful blindness."[58]

The *Inwood* test has served as the touchstone for contributory liability in both real and digital worlds. In *Hard Rock Café Licensing Corp. v. Concession Services, Inc.*, the Seventh Circuit found that the operator of a flea market could be held secondarily liable for a vendor who sold infringing T-shirts, reasoning that the landlord-tenant relationship carried with it special responsibilities to prevent infringement.[59] The Ninth Circuit, too, agreed with this approach in *Fonovisa v. Cherry Auction*, where it applied the *Inwood* test to a swap meet that included counterfeit recordings, reasoning that again, the swap meet provided a marketplace for the sale of the infringing recordings.[60]

These principles have translated uncomfortably to the world of Internet Service Providers (ISP), which in turn creates added instability for platforms. Here, courts have generally followed a proposition advanced by the Ninth Circuit in *Lockheed Martin v. Network Solutions*, which held that if an ISP exercises "direct control and monitoring" over the infringing

55. *Id*. at 846.

56. *Id.* at 854.

57. Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1149 (7th Cir. 1992) ("To be willfully blind, a person must suspect wrongdoing and deliberately fail to investigate").

58. *Id.*

59. *Id.* at 1148–50 (vacating judgment against defendant and remanding to district court for further proceedings as to whether defendant knew or had reason to know of counterfeit sales).

60. Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 265 (9th Cir. 1996) ("*Hard Rock Cafe*'s application of the *Inwood* test is sound; a swap meet can not [sic] disregard its vendors' blatant trademark infringements with impunity. Thus, Fonovisa has also stated a claim for contributory trademark infringement").

conduct, it can be held liable for secondary liability.[61] If the ISP serves as a passive "routing service," like domain name registrars, for example, which links domain names to the IP addresses of their web hosting servers, then the ISP can be immune from claims of contributory liability.[62] If, however, the ISP is able to exercise significant control over the means of infringement, like hosting providers, search engines, or an online marketplace, then the *Inwood* test will apply.[63] If *Inwood* is deemed to apply, the inquiry explores the question of intentional inducement and whether the ISP continued to provide services to an infringer who it constructively or actually knew was infringing.[64]

Both issues are difficult to resolve, however, particularly in the online context. Intentional inducement requires evidence of active involvement by an ISP, and this kind of "smoking gun" evidence is hard to come by.[65] For example, one popular type of trademark infringement lawsuit is in the context of keyword advertising, where plaintiffs allege that defendant ISPs have induced advertisers to infringe plaintiff's marks through the use of keyword suggestion tools.[66] Some courts have held in these situations that there is no inducement because the recommendation is purely algorithmic, leaving the ultimate decision over whether to adopt the keyword in the hands of the advertiser.[67] The same is true for evidence of knowledge by

61. Lockheed Martin Corp. v. Network Sols., Inc., 194 F.3d 980, 984 (9th Cir. 1999) ("Direct control and monitoring of the instrumentality used by a third party to infringe the plaintiff's mark permits the expansion of Inwood Lab.'s "supplies a product" requirement for contributory infringement.").

62. Teague, *supra* note 50, at 471–72.

63. *Lockheed*, 194 F.3d at 984 (adopting the *Hard Rock and Fonovisa* test for contributory liability where an entity has "'suppl[ied] the necessary marketplace'"). Courts have held that each of these types of ISPs could be liable for contributory infringement because they control the infringers' access. *See, e.g.*, Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 104 (2d Cir. 2010) (holding that, while ecommerce websites could be contributorily liable for trademark infringement, eBay was not liable), Louis Vuitton Malletier, S.A. v. Akanoc Sols., Inc., 591 F. Supp. 2d 1098 (N.D. Cal. 2008) (holding a hosting provider contributorily liable for hosting websites that it constructively knew were selling counterfeit products), GEICO v. Google, Inc., 330 F. Supp. 2d 700 (E.D. Va. 2004).

64. *Inwood,* 456 U.S. at 854 (1982).

65. Rian C. Dawson, *Wiggle Room: Problems and Virtues of the Inwood Standard*, 91 IND. L.J. 549, 564 (2016).

66. *See, e.g.*, Rescuecom Corp v. Google Inc., 562 F. 3d 123, 126 (2d Cir. 2009) (describing how Google's suggestion tool works).

67. *See, e.g.*, Rosetta Stone Ltd. v. Google Inc., 730 F. Supp. 2d 531, 539 (E.D. Va. 2010). However, the Fourth Circuit later vacated the decision that had dismissed the contributory liability claims, and remanded the case back to the district court. 676 F.3d

the ISP. Even if an ISP has general knowledge that their service or site is being used to infringe, without specific knowledge of infringement, however, an ISP can generally escape liability, since there is no affirmative duty to actively prevent trademark infringement from occurring.[68]

Although the American approach might appear predictable and uniform, it nevertheless produces unintended consequences. As one commentator has explained, because *Inwood*'s knowledge standards are so unclear, it can lead to an overreaction among platforms, leading to over-responsiveness to trademark owners' notice and takedown requests.[69] In turn, an overreactive impulse carries a disparate impact on small businesses and smaller platforms, who are often ill equipped to defend themselves against potentially false claims of contributory infringement.

Consider a pair of cases, one from the Second Circuit and one from the Ninth Circuit, both influential circuits in the cyber-law space. The first, *Tiffany v. eBay*, decided by the Second Circuit in 2010, involved Tiffany (the luxury jewelry manufacturer) claiming that eBay infringed Tiffany's trademarks by allowing unauthorized sales through the eBay platform. While the court absolved eBay for liability based on its extensive anti-counterfeiting program, it also noted that "[w]hen it has reason to suspect that users of its service are infringing a protected mark, it may not shield itself from learning of the particular infringing transactions by looking the other way."[70] There, the court took great efforts to demonstrate eBay's good faith, illustrated by eBay's immediate actions to not only take down listings that Tiffany declared as infringing, and took affirmative steps to identify and remove counterfeit items.[71] At the same time, it also rejected the idea that a "generalized knowledge that its service is being used to sell counterfeit goods" establishes contributory liability.[72] Instead, the standard

144 (4th Cir. 2012). Rosetta Stone and Google later settled the case. *See* Eric Goldman, *With Rosetta Stone Settlement, Google Gets Closer to Legitimizing Billions of AdWords Revenue*, TECH. & MARKETING L. BLOG (Nov. 5, 2012), http://blog.ericgoldman.org/archives/2012/11/with_rosetta_st.htm. Recent cases involving "hosting" sites adopt a similar stance of active engagement. *See* ALS Scan, Inc. v. Cloudflare, Inc., No. CV 16-5051-GW(AFMx), 2017 WL 1520444 (C.D. Cal. Feb. 16, 2017) (dismissing plaintiff's contributory infringement claim against defendant Steadfast, an ISP host based on a lack of sufficient allegations of inducement).

68. *See Tiffany*, 600 F.3d at 107.

69. Teague, *supra* note 50, at 475–76.

70. *Tiffany*, 600 F.3d at 109.

71. *Id.* at 100.

72. *Id.* at 107.

required some specific knowledge about which listings were infringing or likely to infringe in the future.[73] Because eBay responded promptly to Tiffany's notifications, Tiffany could not satisfy this standard for contributory liability.[74] This decision could be potentially interpreted to require platforms to implement multimillion-dollar anti-infringement programs.[75] This would not only push smaller platforms out of the entry marketplace, but could also push established platforms away from introducing new products, like Amazon.com's product suggestion feature – for fear of facing liability.

The second case, involving Louis Vuitton and Akanoc, a web hosting provider, demonstrates the risk from *not* being over-responsive or not mirroring the multimillion dollar efforts of eBay.[76] In that case, Akanoc, after receiving multiple notices from Louis Vuitton that some of its websites were selling counterfeit merchandise, forwarded the notice to the alleged infringers, rather than take down the sites. In that case, the Ninth Circuit reasoned that Akanoc was serving in a way that was analogous to the Fonovisa flea market operator, noting that hosting websites is the digital equivalent of renting real estate.[77] Because Akanoc had failed to remove the web sites upon notice, the court reasoned that it had been "willfully blind," leading to a 32-million-dollar verdict in favor of Louis Vuitton.[78]

Although the two cases came out differently, they both left a number of questions unanswered, since both failed to specify precisely what actions platforms must take to avoid "shielding itself" from knowledge of infringement. eBay's multimillion dollar VeRo program saved it from millions in infringement damages. The decision in Akanoc seems to imply that this type of program has become the defining standard for all platforms in the future. As Jordan Teague notes,

> [W]hile the eBays of the world can afford to spend millions of dollars combating counterfeiting, this may not be the case for smaller-scale market participants. Requiring 'mom and pop'

73. Stacey L. Dogan, *We Know It When We See It: Intermediary Trademark Liability and the Internet*, 2011 STAN. TECH. L. REV. 7, 8 (2011).

74. *See Tiffany*, 600 F.3d at 110.

75. *See* Teague, *supra* note 50. at 476.

76. Louis Vuitton Malletier, S.A. v. Akanoc Sols., Inc., 658 F.3d 936 (9th Cir. 2011).

77. *Id.* at 942.

78. *Id.* at 947.

> online brokers to wage a million-dollar war against counterfeiting would likely drive these retailers out of business, undesirably narrowing consumer choice.[79]

In attempting to synthesize the cases in this area, Stacey Dogan argues that trademark law reveals great solicitude towards good-faith actors, but reserves the option to condemn trademark intermediaries who might act with the intent or design to sow confusion.[80] Dogan identifies a central synergy between the holdings of *eBay* and those in the copyright context, arguing that the variables of intent, design choices, and commercial motivation help to sort out whether the defendant would be viewed as a "good" or "bad" actor.[81] As she argues:

> Good guys need not redesign their systems or proactively root out infringement that those systems enable; they need only respond to specific instances of infringement that they know about and can stop. They face liability under copyright or trademark law only if they fail to act in the face of such actual knowledge. Bad guys, in contrast, are liable without regard to actual knowledge; having designed their product or service to accomplish unlawful ends, they are charged with the natural consequences of its use. In both copyright and trademark law, then, good guys get the benefits of rigorous liability standards and broad safe harbors; bad guys find themselves in trouble.[82]

For Dogan, the emergence of a fault-based standard for intermediary liability is partially attributable to *Sony*'s dictate to avoid sublimating technological progress to the protection of copyright and trademark law, while recognizing some areas of liability for those whose core business models are specifically designed to enable infringement.[83]

Unfortunately for macrobrands and microbrands, this has led to an environment of uncertainty and tension, which is likely unsustainable as a long-term business strategy. In fact, this lack of certainty led five platform companies – Etsy, Foursquare, Kickstarter, Meetup, and Shapeways – to

79. Teague, *supra* note 50, at 491.

80. Dogan, *supra* note 73, at 6.

81. *Id.* at 8–9.

82. *Id.*

83. *Id.* at 10–11.

advocate for greater certainty in the trademark enforcement area vis à vis platforms.[84] The platforms note in a joint statement that "[a] lack of statutory protections from trademark infringement claims has pushed Commenters to react to many complaints by unquestioningly removing content from their sites. Over the long term, this absence of protection will slow the growth of free expression and commerce that has been the hallmark of the Internet."[85] This Article will revisit the solutions that the platforms propose in Part IV below. Before doing so, it is important to look at how other jurisdictions have been dealing with the same issues in order to learn from their successes and failures.

B. COMPARATIVE APPROACHES: EUROPE AND CANADA

One of the striking features of platforms is their "glocalized" nature—platforms, while global companies, need to rely on local service providers to perform the services.[86] Although there have been efforts at discussing an international liability standard with respect to ISPs, the efforts have not been successful.[87] This has meant that individual jurisdictions have crafted their own rules and standards (as seen in the discussion above in the United States), and so it is important to understand the differing approaches. This Article will look at Europe and Canada, where the questions of liability may be similar, but the answers differ.

1. European Union

Within Europe, the answers to the difficult question of platform liability tends to be grounded in one of three directives: (1) the Electronic Commerce Directive (E-Commerce Directive), adopted in 2000,[88] (2) the Enforcement Directive, adopted in 2004,[89] and (3) the Information Society

84. *See* Etsy, Foursquare, Kickstarter, Meetup, & Shapeways, *Comments in the Matter of Development of the Joint Strategic Plan for Intellectual Property Enforcement* (Oct. 16, 2015) http://extfiles.etsy.com/advocacy/Etsy_IPEC_Comment.pdf.

85. *Id.* at 2.

86. *See* Leah Chan Grinvald, *A Tale of Two Theories of Well-Known Marks*, 13 VAND. J. ENT. & TECH. L. 1, 47 (2010) (discussing glocalization in the context of consumers and trademark perception).

87. Graeme B. Dinwoodie, *Secondary Liability for Online Trademark Infringement: The International Landscape*, 37 COLUM. J.L. & ARTS 463, 467–68 (2014).

88. *See* Council Directive 2000/31, 2000 O.J. (L 178), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32000L0031.

89. *See* Council Directive 2004/48, 2004 O.J. (L 195), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004L0048R%2801%29.

Directive, adopted in 2001.[90] The E-Commerce Directive aims to protect certain types of ISPs from liability (either direct or secondary), whereas the Enforcement Directive and the Information Society Directive may provide different grounds for national courts to hold ISPs liable.

With respect to immunizing certain types of ISPs, the E-Commerce Directive categorizes three types of ISPs: caching, conduit, and hosting.[91] Should the ISP fall within one of these categories, then the ISP would be immune from direct liability of infringement based on its activities with respect to its users.[92] For example, the Court of Justice of the European Union has held keyword advertising programs run by the likes of Google or even eBay are seemingly immune from liability.[93] However, even with the E-Commerce Directive attempting to harmonize the EU member country approach, individual member countries within the European Union have been able to place differing levels of liability on ISPs. For example, France has held that eBay is considered more than a mere "host," which has meant greater responsibility on it to monitor its site for counterfeit products.[94]

In addition, the Court of Justice of the EU has also held that secondary

90. *See* Council Directive 2001/29, 2001 O.J. (L 167), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF; Christiane Wendehorst, *Platform Intermediary Services and Duties under the E-Commerce Directive and the Consumer Rights Directive*, 5 J. EUR. CONSUMER & MKT. L. 30 (2016).

91. Council Directive 2000/31, 2000 O.J. (L 178), Art. 12–14.

92. As one commentator has observed, "The E-Commerce Directive seemed to adopt the basic idea of section 512, namely, a grant of safe harbors from liability for specific intermediary activities, and indeed closely tracked the language of the DMCA in places—particularly with regard to the descriptions of those activities and the conditions for limiting liability." Miquel Peguera, *The DMCA Safe Harbors and their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 COLUM. J.L. & ARTS 481, 482 (2009).

93. Dinwoodie, *supra* note 87, at 482–84 (discussing the Google France and L'Oreal cases). The caveat is that search engines must not have participated actively in the infringement. Case C-324/09, L'Oreal SA v. eBay Int'l AG, 2011 E.C.R. I-6011, P113; P115. This is left up to the national courts to decide. *See id.* There are indications that even using a keyword suggestion tool would be exempt from liability, as German courts have held. *See* Annette Kur, *Secondary Liability for Trademark Infringement on the Internet: The Situation in Germany and Throughout the EU*, 37 COLUM. J.L. & ARTS 525, 531 (2014).

94. Teague, *supra* note 50, at 473. *See also* Peguera, *supra* note 92, at 499–512 (discussing a number of other European court cases along similar lines, including the French *eBay* case).

liability standards are to be assessed at the national level.[95] This now allows each member country to apply its own laws with respect to secondary liability, which do differ. For example, the United Kingdom has a more stringent standard to meet in order to be liable as an "accessory," whereby a plaintiff must prove that the defendant "conspired with the primary party or procured or induced his commission of the tort . . . ."[96] This is contrasted with Germany, which takes a slightly less stringent approach, finding liability if there was a "willful adequate causal contribution to the infringing acts of any third party; the legal and factual possibility of preventing the resulting direct infringements; and the violation of a reasonable duty of care to prevent these infringements."[97]

Even though the European Union has introduced "notice-and-action" procedures, these are not formalized.[98] As such, much of the procedures that are in place are privately regulated, such as the efforts of the European Commission working with brand owners and Internet platforms regarding the sale of counterfeit goods.[99] However, even with these informal procedures, combined with the legal uncertainty across European Union member countries of the application of the E-Commerce Directive safe harbors, ISPs are leery of taking additional measures that may lead to more "effective self-regulatory measures."[100]

---

95. *See* Case C-238/08, Google France v. Louis Vuitton Malletier S.A., 2010 E.C.R. I-2467, Para 107, I-2511., http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62008CJ0236.

96. Dinwoodie, *supra* note 87, at 485 (quoting L'Oreal SA v. eBay Int'l AG, 2011 E.C.R. I-6011).

97. Matthias Leistner, *Structural Aspects of Secondary (Provider) Liability in Europe*, 9 J. INTELL. PROP. L. & PRAC. 75, 78–79 (2014).

98. *See* Council Directive 2000/31, 2000 O.J. (L 178) on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN. (obligating member states to exempt intermediaries from liability in situations listed in Section 4, but not requiring any specific "notice and action" procedure, like in the DMCA). Except some member states have enacted provisions statutorily, like France. *See* Peguera, *supra* note 92, at 490–91.

99. *See* EUROPEAN COMMISSION, ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS https://ec.europa.eu/growth/industry/intellectual-property/enforcement_en (describing the European Commission's efforts in coordinating voluntary agreements among brand owners).

100. European Economic and Social Committee and the Committee of the Regions, *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe* (May 25, 2016) at 9, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288.

2. Canada

In Canada, the picture is less clear than in the European Union and the United States. As a relatively small market, Canada has seen comparatively little litigation about trademarks and platform liability.[101] This could be due to the smaller percentage of Canadians who have used such platforms, as compared to Americans, or that Canada is simply a smaller market than the United States.[102] In the area of keyword advertising, where litigation in the United States has been quite active, Canada had its first case only in 2015.[103] And even in this case, the litigation was between two competitors regarding whether the defendant's purchase of the plaintiff's trademarks as keywords was likely to confuse Internet users.[104] Another reason for the lack of intermediary trademark infringement lawsuits is that Canada does not have a secondary liability regime for online uses of trademarks.[105]

However, this may be changing, as a recent case involving Google's role as a global search engine shows. In *Google v. Equustek Solutions*,[106] the defendants had previously been found to be guilty of passing off its electronic devices as the plaintiff's.[107] The lower court judgment had

101. For example, one commentator has compared Canada's 2014 Gross Domestic Product to that of the state of Texas. *See* Mark J. Perry, *Putting the Ridiculously Large $18 Trillion US Economy Into Perspective by Comparing State GDPs to Entire Countries*, AEIDEAS, (June 10, 2015), http://www.aei.org/publication/putting-the-ridiculously-large-18-trillion-us-economy-into-perspective-by-comparing-state-gdps-to-entire-countries/.

102. For a quick comparison (but not necessarily scientific), compare http://www.statcan.gc.ca/daily-quotidien/170228/dq170228b-eng.htm (Canada) with http://www.pewinternet.org/2016/05/19/the-new-digital-economy/ (U.S.).

103. Michelle Kerluke, *Canadian trademarks and keyword advertising: the unsettled debate over trademark keywords*, PhD diss., Univ. of British Colum. (2016), http://hdl.handle.net/2429/58805, at ii.

104. Vancouver Community College v. Vancouver Career College (Burnaby), 2015 BCSC 1470.

105. *See* Michael Geist, *No Monitoring & No Liability: What the Supreme Court's Google v. Equustek Decision Does Not Do,* MICHAEL GEIST (Jun. 29, 2017) http://www.michaelgeist.ca/2017/06/no-monitoring-no-liability-supreme-courts-google-v-equustek-decision-not (discussing the response to the Equustek decision by the music industry, which interpreted the Canadian Supreme Court to hold that "facilitating" infringement was liable in Canada, an interpretation that Professor Geist believes is incorrect).

106. Google Inc. v. Equustek Solutions Inc., 2017 S.C.C. 34, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do.

107. Equustek Solutions Inc. v. Jack, 2014 BCSC 1063, https://www.canlii.org/en/bc/

ordered the defendant to stop its sales, however, the defendant did not comply. Google, which was not a party to the lawsuit, had removed the defendant's websites from the search results that would show up in a search on google.ca, but Canadians could still access defendant's websites on other Google sites. This led the plaintiff to ask the court to compel Google to block the defendant's sites on a global basis, which it granted.[108]

The secondary liability implications stem from the lower court's statement that, "Google is an innocent bystander but it is unwittingly facilitating the defendants' ongoing breaches of this Court's orders. There is no other practical way for the defendants' website sales to be stopped. There is no other practical way to remove the defendants' websites from Google's search results."[109] Google appealed the case all the way to the Canadian Supreme Court.[110] Although most commentators have focused on the free speech and forum-shopping implications stemming from Canadian Supreme Court decision,[111] language that the Supreme Court

bcsc/doc/2014/2014bcsc1063/2014bcsc1063.html. In this case, defendants had been former distributors of plaintiffs' products and were accused of a number of infringements of the plaintiffs' intellectual property. First, defendants were accused of using the plaintiffs' trade secrets to design and manufacture a similar product that competed with the plaintiffs'. In addition, before selling their own product, defendants passed off plaintiffs' products as their own by covering up the trademarks on the actual product. And in selling their own product, defendants advertised using plaintiffs' products, but would deliver orders using their own product. *Id*. at paras 3–9.

108. *Equustek*, 2014 BCSC 1063, at paras 10, 159.

109. *Id.* at para 156.

110. *Google Inc*.., 2017 S.C.C. 34, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do.

111. Mike Masnick, *Canadian Supreme Court Says It's Fine To Censor The Global Internet; Authoritarians & Hollywood Cheer*, TECHDIRT (June 28, 2017), https://www.techdirt.com/articles/20170628/11273937689/canadian-supreme-court-says-fine-to-censor-global-internet-authoritarians-hollywood-cheer.shtml; Howard Knopf, Google Suffers Severe Setback from the Supreme Court of Canada, Excess Copyright (June 28, 2017), http://excesscopyright.blogspot.ca/2017/06/google-suffers-severe-setback-from.html; EFF, *Top Canadian Court Permits Worldwide Internet Censorship* (Jun. 28, 2017), https://www.eff.org/deeplinks/2017/06/top-canadian-court-permits-worldwide-internet-censorship; Daphne Keller, *Ominous: Canadian Court Orders Google to Remove Search Results Globally*, CTR. FOR INTERNET & SOC'Y BLOG (Jun. 28. 2017) http://cyberlaw.stanford.edu/blog/2017/06/ominous-canadian-court-orders-google-remove-search-results-globally; Michael Geist, *Global Internet Takedown Orders Come to Canada: Supreme Court Upholds International Removal of Google Search Results*, MICHAEL GEIST (June 28, 2017), http://www.michaelgeist.ca/2017/06/global-internet-takedown-orders-come-canada-supreme-court-upholds-international-removal-google-search-results/.

uses does appear to support opening the door to secondary liability in the online trademark infringement context.[112] In fact, the Canadian music industry appears to have interpreted the Supreme Court language in this manner, issuing a press release that celebrates the decision.[113] However, there are varying interpretations, in particular, Michael Geist's counter-argument that the Supreme Court did not open this door.[114]

Notwithstanding these developments in secondary liability, there is a parallel claim of negligence for failing to act on knowledge of wrongdoing that could be made. The kernel of this argument is found in *Louis Vuitton v. Lin*, where a landlord was held liable for knowingly allowing counterfeit products to be sold at their premises.[115] Similar to the "swap meet" cases of *Hard Rock* and *Fonovisa* in the U.S. discussed above, the court held that the landlord had a duty to investigate serious allegations of wrongdoing.[116] While this argument has not been made with respect to platforms, some commentators believe that this line of reasoning could be plausibly extended to the online context.[117] However, given the application by U.S. courts of the swap meet cases to platform infringement cases, this does seem like it can be a likely extension by the Canadian courts in the future.

---

112. *Google Inc*.., 2017 S.C.C. 34, at para 53 ("This does not make Google liable for this harm. It does, however, make Google the determinative player in allowing the harm to occur."). *See also* Adam Bobker & Janice Calzavara, *Leave to Appeal to SCC: Google Inc v Equustek Solutions Inc (BCCA)*, BERESKIN & PARR (Mar. 7, 2016) http://www.bereskinparr.com/index.cfm?cm=Doc&ce=downloadPDF&primaryKey=733 (discussing the lower court case).

113. Press Release, Music Canada, Music Canada applauds Supreme Court of Canada decision confirming that Internet intermediaries can be ordered to deindex illegal sites worldwide (June 28, 2017) https://musiccanada.com/news/music-canada-applauds-supreme-court-of-canada-decision-confirming-that-internet-intermediaries-can-be-ordered-to-deindex-illegal-sites-worldwide/ ("Today's decision confirms that online service providers cannot turn a blind eye to illegal activity that they facilitate; on the contrary, they have an affirmative duty to take steps to prevent the Internet from becoming a black market.").

114. *See* Geist, *supra* note 105 ("The music industry may have wanted the Supreme Court of Canada to establish an affirmative duty on Google to monitor content, but the ruling is unequivocal that there is no such requirement as a result of the Equustek decision.").

115. This was a procedurally complicated case, with the first case holding in favor of Louis Vuitton on a default judgment. 2007 FC 1179 (CanLII). The second case was where the defendant asked the court to set aside the default judgment. 2008 FC 45.

116. 2008 FC 45, ¶16.

117. *See* James L. Bikoff et al., *Hauling in the Middleman: Contributory Trade Mark Infringement in North America*, 5 J. INTELL. PROP. L & PRAC. 332, 340 (2010).

***

The existing situation becomes somewhat circular: because of the indeterminacy of the law, many parties have resorted to out-of-court settlements as a more viable option, leaving many gaps and stasis in existing common law frameworks.[118] In addition, operating in the "shadow of the law" leaves many smaller business entities and individuals vulnerable to legal claims that may or may not be accurate representations of more well-resourced entities' legal rights.[119] At the same time, solely leaving these issues up to legislative bodies can result in a statutory framework that may leave little room for judicial refinement, overlooking the importance of restoring frameworks to protect innovation and dynamism, a point this Article returns to in Part IV.[120]

III. PLATFORM DECENTRALIZATION AND THE MICROBRAND

On the platform, everyone gets to be an entrepreneur. Scholars have written extensively about the culture of "micro-entrepreneurship," particularly in the developing world.[121] In some countries, like Bolivia, for example, individuals engage in entrepreneurial activities at three times the rate in the United States.[122] Such entrepreneurial engagement also creates opportunities for small and medium-size businesses to market themselves more effectively, particularly since the platform economy can function as a powerful tool for digital marketing.[123] App builders can create on platforms like Android, iOS, Amazon Web Services, and others.[124] Idle time can be taken up by serving as a driver for Lyft or Uber, vacant space by renting on Airbnb. Some individuals, virtually, provide goods through platforms like app stores, YouTube, or Amazon self-publishing. Agencies cater to "influencers" on YouTube, transforming individuals into stars with substantial followings. Irrespective of the specific platform, all of them direct themselves towards a single goal: encouraging everyone to

118. Teague, *supra* note 50, at 484–85.

119. *See* Leah Chan Grinvald, *Policing the Cease-and-Desist Letter*, 49 U.S.F. L. REV. 409, 412 (2015).

120. *See* Teague, *supra* note 50, at 485.

121. Karl Loo, *How the Gig Economy Could Drive Growth in Developing Countries*, FORBES (Mar. 23, 2017, 12:04PM) https://www.forbes.com/sites/groupthink/2017/03/23/how-the-gig-economy-could-drive-growth-in-developing-countries/#3db6d56a4a49.

122. *Id.*

123. *Id.*

124. Kenney & Zysman, *supra* note 2, at 1.

contribute.[125] The most optimistic picture, then, suggests that the everyday individual can be readily transformed into an entrepreneur, able to take advantage of scheduling flexibility and able to monetize their personal and professional assets towards this goal.[126]

In turn, the mini-entrepreneur facilitates the emergence of the microbrand. Even in digital space, platforms enable the transformation of an everyday citizen into a brand. As one study observes, "[t]he similarities between the online presentation of people and products, individuals and brands, are striking: the same interfaces and tactics apply to both, making them even more exchangeable than before."[127] Some people have lives on social media for the purposes of communication, others for the purposes of promotion, connection, and still others for the purposes of expression.[128] Yet a platform's marriage to self-branding transforms and synergizes all of these purposes into one singular purpose of micro-entrepreneurship.

Even in this context, however, the governing indeterminacy over contributory liability contributes to a particular confusion even within the microbrand ecosystem. This next Part explores how the existing frameworks of contributory liability contribute to a growing divide between small and large entities, and show how the architecture of platforms contributes to this disparate impact.

A. MICROENTREPRENEURSHIP AND THE MICROBRAND

Nearly every prominent platform encourages the "self-branding" of entrepreneurs, enabling ordinary citizens to essentially become corporate entities by building a consumer following. Much of these views are inextricably linked to a conception of the self that is intertwined with the idea of commodification. Under this approach, linked to the idea of "possessive individualism," we all own ourselves, as property, and therefore our capacity to contribute is linked metaphorically to the notion of property.[129]

Airbnb, for example, explicitly uses language about creating a micro-brand: "Your brand, or micro-brand, is what makes your listing unique and helps you stand out from the competition. Branding your listing is of

125. *Id.* at 2.

126. *Id.*

127. José van Dijck, *'You have one identity': performing the self on Facebook and LinkedIn*, 35 MEDIA, CULTURE & SOC. 199, 207 (2013).

128. *Id.* at 211.

129. Ilana Gershon, *Selling Your Self in the United States, Political and Legal*, 37 ANTHROPOLOGY REV. 281, 288 (2014).

utmost importance! Proper branding ensures that your listing resonates with your target market and attracts ideal guests."[130]

In another typical example, a pair of Brown University students started a company, Teespring, that will only agree to produce shirts when pre-orders reach a minimum threshold, thereby eliminating risk for the average producer, enabling them to scale production quickly and effectively.[131] The model is again a "microbrand": the production of "products that are tailored towards individual affinities[,] rather than consumption for the mass market."[132] The company has received tens of millions in venture capital financing, and hundreds have earned more than six figures from their micro-production (not including launching at least ten millionaires).[133] In another context, some entrepreneurs in the consignment economy have grown so large that they have received venture capital investment.[134]

Even when some kinds of mini businesses are not known for their profit, they still create new formations of platform entrepreneurship.[135] Influencers, for example, have been touted as the new brands, described as "the golden children of marketing strategies right now."[136] Some studies argue that consumers trust influencers far more than they trust advertisements or even celebrity endorsements.[137] Here, too, platforms have emerged to provide a springboard to match influencers with particular brands.[138] MuseFind, for example, exists as a platform that assists brands to find relevant influencers for their target audience, and then monitors their performance in marketing a brand.[139] Often, the effectiveness of an influencer campaign depends on how "authentically"

130. AIRBNB GUIDE, *Good Design is Good Business* https://www.airbnbguide.com/good-design-is-good-business/.

131. Marcus Wohlsen, *These Guys Made a T-Shirt. Now Silicon Valley Is Giving Them Millions*, WIRED (Nov. 18, 2014) https://www.wired.com/2014/11/guys-made-t-shirt-now-silicon-valley-giving-millions-2/.

132. *Id.*

133. *Id.*

134. Kenney & Zysman, *supra* note 2, at 66.

135. *Id.*

136. Deborah Weinswig, *Influencers are the New Brands*, FORBES (Oct. 5, 2016, 9:30AM) https://www.forbes.com/sites/deborahweinswig/2016/10/05/influencers-are-the-new-brands/#618c60217919.

137. *Id.* (citing study by MuseFind that shows 92% of consumers trust influencers more than other forms of marketing).

138. *Id.*

139. *Id.*

she is viewed by the target audience, leveraging an economy of trust between the consumer and the influencer.[140]

Alice Marwick, in her book Status Update, explains that the concept of "self-branding" has become an essential Web 2.0 strategy, something that is firmly instilled in today's business culture.[141] The idea, at its simplest, is to match marketing strategies with the individual entrepreneur, "a way of thinking about the self as a salable commodity that can tempt a potential employer."[142] Social media, here, is essential to enable widespread self-promotion.[143] She quotes an article by Tom Peters that appeared in FAST COMPANY, titled "The Brand Called You," that relates:

> The main chance is becoming a free agent in an economy of free agents, looking to have the best season you can imagine in your field, looking to do your best work and chalk up a remarkable track record, and looking to establish your own micro equivalent of the Nike swoosh. . . . The good news—and it is largely good news—is that everyone has a chance to stand out. Everyone has a chance to learn, improve, and build up their skills. Everyone has a chance to be a brand worthy of remark.[144]

Here, several factors—the rise of megacorporate brands, coupled with an entrepreneurial mindset and project-based work cultures—all contribute to the individualistic, decentralized world of the microbrand.[145]

In some cases, because microbranding is linked to a changeable, fluid, human personality, as opposed to a fixed product, it creates new vulnerabilities, requiring even greater brand management, surveillance and enforcement.[146] Some individuals set up Google alerts to let them know when they are mentioned online; others use Twitter and other software to let them know when they are being replied to or retweeted; others spend

140. *Id.*

141. ALICE E. MARWICK, STATUS UPDATE 164 (2013).

142. *Id.* at 166.

143. *Id.*

144. *Id.* at 165 (quoting Tom Peters, *The Brand Called You*, FAST COMPANY (Aug. 31, 1997) https://www.fastcompany.com/28905/brand-called-you).

145. *Id.* At the same time, however, as Marwick warns us, the benefits of self-branding can tend to privilege a certain demographic—white, wealthy males who have considerable independence relative to female or minority demographics, who may have less flexibility to devote time to self-branding opportunities. *See id*. at 180–81.

146. Gershon, *supra* note 129, at 290.

hours combing social media looking for references to their name or brand.[147] Marwick quotes Glenda Bautista, who served as head of product for video at AOL who describes an endless chain of self-policing and policing of others, constantly asking others to take photographs, and peppering commentary with references to high-status individuals, even when their relationships are remote.[148] As Marwick explains, this process "requires continually imagining oneself through the eyes of others, creating a 'dual gaze' of internalized surveillance."[149] Through this process of surveillance and monitoring, self-branding produces an "edited self," someone who appears to be "an entrepreneur whose product is a neatly packaged, performed identity."[150] In other contexts, like Uber, entrepreneurs are incentivized through ratings and other reputational tools to encourage effective performance, unlike cab drivers who are typically anonymous and unknown to the passenger.[151]

While at first glance it may seem that self-branding and trademark law rarely intersect, the truth is that they draw upon similar concerns regarding property, identity, and association. The endless cycle of self-branding and brand monitoring affects trademark enforcement in two primary ways. First, it may incentivize microbrands to spend significant resources of time and money to enforce their trademarks, due in part to the constantly changing brand environment they inhabit. Second, the constant pull of brand monitoring may lead macrobrands, in turn, to internalize the same range of additional costs faced by microbrands, leading, again, to trademark surveillance and overenforcement. Finally, these disparities in turn, can contribute to a widening divide between smaller and larger platforms that may have different abilities and resources to address enforcement, thus impacting the path of platform innovation.

B. MICROBRANDING AND CONTRIBUTORY LIABILITY

In the context of platforms, many scholars and commentators have raised the question of whether there is a hierarchical distinction between the "platform owner" and the entrepreneurs and contractors that facilitate

147. Marwick, *supra* note 141, at 190.

148. *Id.* at 190–91.

149. *Id.* at 191.

150. *Id.* at 195.

151. Jonathan V. Hall & Alan Krueger, *An Analysis of the Labor Market for Uber's Driver-Partners in the United States* 32 (Nat'l Bureau of Econ. Research, Working Paper No. 22843).

this economy.[152] The same question, we argue, might also be posed in the trademark arena, that is, whether our system of contributory liability, as well intended as it might be, facilitates the formation of an unequal system that extends the benefits of trademark protection and enforcement to a few, but radically undervalues the contributions of the mini entrepreneurs that characterize platform vitality. The absence of statutory safe harbors in the trademark context often has a particularly deleterious effect on smaller ISPs and related platforms, who may face different challenges based on their limited legal resources.[153] Many smaller ISPs do not have automated systems to respond to 512 notices, and therefore an attention to the diversity of ISP platforms is especially critical in considering how to design better systems of notification and enforcement.[154]

According to Stacey Dogan, existing trademark frameworks unwittingly encourage aggressive behavior through two central mechanisms.[155] The first involves the oft-mentioned trope that trademark owners must police their marks.[156] The existing lack of clarity regarding trademark owner's duty to police can lead to overenforcement, lending further strength to the perception that "stronger" marks receive more protection, and "weaker" marks get less. As Dogan explains, although trademark owners are required to take certain steps to enforce their marks, the confusion regarding the required level of notice to prospective defendants encourages them to take an "object first, analyze later" approach.[157] As a result, many trademark owners take an approach that objects to all third party uses of their marks, even when confusion does not result.[158] Dogan concludes, therefore, that many cases of trademark bullying involves value maximizing choices—trademark owners object, not because they risk "losing their marks if they fail to object, but because their rights will be more valuable if their objection succeeds."[159]

Consider dilution protections, as one example. Even though the

152. Kenney & Zysman, *supra* note 2, at 67.

153. *See* Kickstarter, Makerbot, Meetup, & Shapeways, *Additional Comments in the Matter of Section 512*, Docket No. 2015-7, at 3 (Feb. 23, 2017).

154. *See id.*, at 3–4.

155. Stacey Dogan, *Bullying and Opportunism in Trademark and Right-of-Publicity Law*, 96 B.U. L. REV. 1293, 1318 (2016).

156. *Id.* (explaining that, in reality, their responsibilities are much more limited—they do not lose their rights by failing to object to uses that are non-infringing).

157. *Id.* at 1318–19.

158. *Id.* at 1319.

159. *Id.*

strongest, most famous marks carry the least risk of losing their distinctiveness, the law's existing framework directs courts to consider the extent to which a mark holder engages in "substantially exclusive use of the mark," thereby indirectly encouraging trademark holders to overpolice their marks to satisfy this standard.[160] Similar concerns regarding exclusivity also carry over into the standard for infringement, as well. This leads trademark owners to police their marks for anything remotely appearing similar, as a function of preserving the value of a mark, rather than guarding against a true risk of confusion.[161]

These harms become even more apparent when we turn to the architecture of platforms. Due to the absence of trademark safe harbors, ISPs cannot institute a counter notice procedure for solely trademark-related claims; and as a result, users do not have the ability to challenge the notification and keep their work online.[162] Etsy, for example, has observed that its number of trademark-related takedown notices is greater than the copyright-related ones that it has received.[163] It offers examples of the notices it has faced: one involving a graphic designer using the trademarked name of a television show on a set of custom party invitations; an artist using a trademarked cartoon character in a humorous oil painting; or a small business owner who repackages food packaging into purses and liquor bottles into drinking cups.[164] Even though each of these instances might be the subject of strong arguments for non-infringing uses, each of them was the subject of a takedown notice.[165]

Because of the absence of clear safe harbors in the ISP context with respect to trademark law, commentators have argued that many ISPs will not challenge trademark requests in order to avoid becoming embroiled in costly litigation.[166] As a recent filing by Etsy and other platforms concluded, "[t]he result is that a trademark claim – even one built on a weak foundation – can be an effective way to permanently quash the

160. *Id.*

161. *Id.* at 1321 (quoting 2 J. THOMAS MCCARTHY, MCCARTHY TRADEMARKS AND UNFAIR COMPETITION § 11.91 (4th ed.): "[t]he only way a trademark owner can prevent the market from being crowded with similar marks is to undertake an assertive program of policing adjacent 'territory' and suing those who edge too close").

162. *See* Etsy, Foursquare, Kickstarter, Makerbot, Meetup, Shapeways, & Stratasys, *Comments in the Matter of Section 512*, Docket No. 2015-7, at 3 (Apr. 1, 2016).

163. *Id.* at 3.

164. *See* Etsy, et al., *supra* note 84, at 3.

165. *Id.*

166. *See* Etsy, et al., *supra* note 162, at 3.

speech or economic activity of others."[167] In such cases, because of the complexity of trademark law, and the David vs. Goliath status of the user vs. the trademark owner, respectively, ISPs may not even provide the user with an opportunity to challenge the assertion of infringement.[168] Here, small businesses, individual entrepreneurs, and ordinary creators might be most affected by such notices, simply because they lack the resources and channels to challenge their targeting.[169] And smaller ISPs, since they may be unable to afford the legal resources required to investigate a claim, may err on the side of over-accommodation as a result.[170] Over the long term, these abusive practices can have the effect of actually undermining support for intellectual property altogether. As Etsy and others have noted, "[a] steady stream of examples of abuse can reduce the legitimacy of rightsholders as a whole in the eyes of the public, thus reducing public support for enforcement even in legitimate cases of infringement."[171]

Further, because of the absence of trademark-related safe harbors, many platforms have reported situations where a rightsholder conflates both copyright and trademark-related requests in the same notice, knowing that the absence of a safe harbor in trademark requests will make it much more likely that an ISP will respond by taking down the content.[172] For example, a rightsholder might object to content that includes a character (protected by copyright) and its name (that is protected by trademark).[173] The 3D printing company, Shapeways, for example, has found that in 2015, 76% of the copyright takedowns include trademark-related claims.[174] A year later, Shapeways noted that although the number of overlap claims had significantly reduced overall, it still found that the majority of its most defective takedown claims were trademark-related.[175]

Yet consider the result of this overlap. Since Shapeways does not generally accept counter notices for non-copyright claims, this means that the majority of its users targeted by takedown requests are unable to

167. *See id.*

168. *See id.*

169. *See id.* at 4.

170. *See id.*

171. *See id.* at 5.

172. *See Etsy, et al.*, *supra* note 162, at 5.

173. *Id.* ("For example, a rightsholder may request the removal of user content consisting of a copyright-protected character and its trademark-protected name.").

174. *See* SHAPEWAYS, 2016 Transparency Report, at https://www.shapeways.com/legal/transparency/2016.

175. *See id.*

respond to these allegations.[176] As a result, this loophole essentially enables a rightsholder to evade the counter-notice requirements under the DMCA, since trademark law does not allow for the same process, thereby risking overenforcement and abuse.[177] "Even if a user intends to challenge the copyright portion of the request, the trademark portion often remains unchallengeable, resulting in the targeted content staying down."[178] Since the vast majority of such cases are resolved privately, "OSPs are largely left to create their own patchwork of policies, hoping that their decisions strike a reasonable balance between enforcement and expression. This results in an uneven, largely undocumented shadow dispute resolution process that breeds an under appreciation for the scope of the problem and a lack of uniform rules to help guide their resolution," commentators observe.[179]

In such cases, it is important to distinguish between abusive trademark enforcement and enforcement that seeks to execute legitimate trademark rights.[180] While the latter goal is clearly deserving of support, the former scenario – overenforcement – has a deleterious effect on startups and smaller platforms that may lack the resources to respond properly to a dispute. In such situations, the assertion of overbroad trademark rights, facilitated by an overreliance on automated systems of enforcement, may produce false positives without significant human oversight.[181] In some cases, these complaints can be sent by a rightsholder who uses these notices to undermine a competitor or to censor critical commentary.[182] For example, a recent filing noted an incident where a political action committee requested a takedown of material that parodied Hilary Clinton's campaign logo.[183] Or a similar situation where another candidate, Ben Carson, requested takedown requests regarding merchandise that used Carson's name on items relating to his candidacy.[184] Often, these claims involve a mixture of trademark and copyright claims, further muddying the waters of potential defenses, but

176. *See id*.
177. *See id*.
178. *Etsy, et al.*, *supra* note 162, at 5.
179. *Id.* at 5.
180. *See id*. at 2.
181. *See* SHAPEWAYS, *supra* note 175.
182. *See id*.
183. *See id*. at 3.
184. *See id*.

they can often involve politically oriented speech worthy of protection.[185] The collective effect of these claims, however, limits the potential circulation of the free flow of information and ideas, further amplifying how smaller platforms become implicated in a system of overbroad (and inconsistent) regulation.

IV. REFORMING PLATFORM ARCHITECTURE THROUGH TRADEMARK MODERNIZATION

Platforms, then, present us with a curious paradox: as much as platforms disrupt conventional business models and challenge classic assumptions about regulation, they also can enable a rise in regulation characterized by increases in permitting, licensing, and protection.[186] In other words, the absence of law facilitates the rise of platforms, but the rise of platforms requires a regulatory system to sustain its growth. In sum, at the same time that platforms challenge established theories of the market, they also facilitate increased regulation.

The same can also be said regarding how our intellectual property system intersects with platform architecture. Particularly regarding trademark law, platforms provide us with the opportunity to look for ways to harmonize the interaction of microbrands and macrobrands while encouraging the development and protection of platform enterprises. As Rob Merges has argued in the platform context, intellectual property rights confer on their owners merely an *option* to enforce their rights.[187] This suggests that at times, the law may need to regulate the ex post policing of intellectual property enforcement in flexible and careful ways to ensure a balance between competition and regulation.[188] Drawing in part from these observations, this final Part explores a number of ways in which trademark law can be modernized to better address the challenges presented by platform architecture. Here, acknowledging that there is no "silver bullet" to resolve these complex issues, this Article analyzes a variety of potential improvements to the law from different angles. While change can occur by legislation or through an adoption of voluntary measures by platforms themselves, this Article's suggestions include the formation of statutory safe harbors among platforms, a "notice-and-notice" system, as well as a

185. *See id*.

186. Lobel, *supra* note 1, at 90.

187. *See* Robert P. Merges, IP Rights and Technological Platforms 18 (Dec. 1, 2008), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1315522.

188. *See id*. at 10.

variety of changes to the common law, including the application of a materiality of harm requirement and clarification of the duty to police.

A. SAFE HARBORS

"True" statutory safe harbors are rare in trademark law.[189] By "true" we mean categories of unauthorized trademark use that is deemed to be non-infringing, or what some commentators refer to as "categorical exemptions."[190] This has likely been a conscious decision, as judges to date have been lukewarm to the idea of categorical exemptions or "bright line rules" in trademark law.[191] The reason for this is that trademark law has traditionally been context-driven, with a focus on minimizing, or avoiding altogether, consumer confusion.[192] Any attempts by judges to create shortcuts through the lengthy, time-consuming, and expensive analysis of the likelihood of confusion have been met with resistance.[193]

189. This is the case, except for two very narrow statutory safe harbors for "innocent" publisher or domain name registrar. 15 U.S.C. §1114(2). One could argue that the exclusions from actionable dilution in Section 43(c)(3) of the Lanham Act are akin to a safe harbor. However, it is a very narrow one, limited to nominative or descriptive fair use in comparative advertising or social commentary (like parody, satire or criticism), news reporting, or any noncommercial use. 15 U.S.C. § 1125(c)(3). However, these types of uses may still be subject to trademark infringement claims. In addition, there is still the potential for a dilution claim where a judge determines that the defendant's use is not within one of these categories. *See, e.g.*, Louis Vuitton Malletier, S.A. v. Hyundai Motor Am., No. 10 Civ. 1611 (PKC), 2012 WL 1022247, *16–*20 (S.D.N.Y. Mar. 22, 2012) (finding in favor of plaintiff Louis Vuitton that defendant Hyundai did not use the Louis Vuitton marks within the scope of one of these exceptions and had no intent to do so). *See also* William McGeveran, *Rethinking Trademark Fair Use*, 94 IOWA L. REV. 49, 104–109 (2008) (providing a critique of the dilution safe harbor).

190. William McGeveran, *The Trademark Fair Use Reform Act*, 90 B.U. L. REV. 2267, 2272 (2010); Lisa P. Ramsey, *Increasing First Amendment Scrutiny of Trademark Law*, 61 SMU L. REV. 381 (2008).

191. McGeveran, *supra* note 190, at 2268 ("Traditionally, trademark law has eschewed per se exceptions").

192. Leah Chan Grinvald, *Shaming Trademark Bullies*, 2011 WIS. L. REV. 625, 658 (2011).

193. For example, in *Vornado Air Circulation Systems, Inc. v. Duracraft Corp.*, where the Tenth Circuit attempted to draw a somewhat bright line where the existence of a utility patent on a product configuration would prevent trade dress. 58 F.3d 1498 (10th Cir. 1995) ("Where disputed product configuration is part of claim in utility patent, and configuration is described, significant inventive aspect of the invention, so that without it the invention could not fairly be said to be the same invention, patent law prevents its protection as trade dress, even if configuration is nonfunctional."). The Supreme Court blurred this bright line in *TrafFix Devices, Inc. v. Marketing Displays, Inc.* by turning the rule into a part of the evidentiary assessment. 532 U.S. 23, 29 (2001) ("A utility patent is

However, there is a real need for such categorical exemptions in trademark law, particularly in today's world of "trademarking everything"[194] in the online world. As noted previously, some platforms themselves have argued for the need for safe harbors (as well as for a better defined system within which to operate, which we address below in our "notice-and-notice" proposal) due to the overwhelming nature of trademark infringement notices that may or may not be valid.[195] These platforms have argued that the creation of statutory safe harbors would increase accountability and public awareness, as well as encourage a greater uniformity of guiding principles to address trademark disputes in the ISP context.[196]

But a categorical exemption would also benefit macro- and micro-brands in particular ways. On the macrobrand side, it would mean that platforms are no longer required to respond to every instance of perceived infringement. In addition, macrobrands would be able to provide clearer guidance to the microbrands within their ecosystem about what is and what is not acceptable.[197] Since most of the trademark disputes occur extra-judicially, having clear guidelines would assist all within the platform ecosystem in deciding which claims are valid, and which involve trademark over-enforcement (and perhaps even bullying).

In terms of specific categorical exemptions, there is a rich body of literature already on the topic, as we are not the first scholars or commentators to argue for trademark safe harbors. Due to space limitations, we will mention just a few here as examples.[198] Eric Goldman has called for a safe harbor for Internet search providers, which would exempt such search providers from infringement liability for activities like keyword advertising.[199] Lisa Ramsey has argued that categorical safe

---

strong evidence that the features therein claimed are functional").

194. *See generally* Lisa P. Ramsey, *Trademarking Everything? Why Brands Should Care About Limits on Trademark Rights*, presentation at The 2015 Works-in-Progress Intellectual Property Colloquium, United States Patent & Trademark Office, Alexandria, VA (Feb. 6, 2015).

195. *See* Etsy, et al., *supra* note 162, at 2.

196. *See id.*

197. Some platforms do try to provide guidance. *See, e.g.*, Etsy.com, https://www.etsy.com/teams/7722/discussions/discuss/13810041/.

198. Due to space, we are not able to discuss all the many innovative proposals here. On safe harbors, see Ramsey, *supra* note 190, at 455–56. (arguing for categorical safe harbors to protect speech); Eric Goldman, *Deregulating Relevancy in Internet Trademark Law*, 54 EMORY L.J. 507 (2005) (arguing for safe harbors for Internet search providers).

199. Goldman, *supra* note 198, at 588–595.

harbors should be legislatively adopted for certain uses of trademarks, or even for certain types of defendants, such as ISPs.[200] Bill McGeveran has crafted and argued for an entire "Trademark Fair Use Reform Act" that would exempt trademark uses within communicative works from both infringement and dilution claims.[201]

Unfortunately, though, categorical exemptions would really only work for the clear-cut cases. There are many uses of trademarks that fall in the middle and for this, we would propose a new system for trademark owners, macrobrands, and microbrands, to use in the online platform ecosystem.

B. "NOTICE AND NOTICE"

The secondary liability standard is one of the leading causes for platform uncertainty in dealing with claims of trademark infringement, as we outlined above. Exacerbating this uncertainty is a lack of a second type of safe harbor (as opposed to the first type that we just discussed, categorical exemptions), one that would immunize platforms and other online entities from any trademark infringing behavior by their users. As Part III mentions, "notice and takedown" has become the unintentional default regime for trademark claims (even though the DMCA only applies to claims of copyright infringement) because copyright owners are including claims of trademark infringement within the same notice to the ISPs.[202] Particularly after the Second Circuit decision in *eBay*, platforms are extremely reluctant to ignore the trademark claims, even where the platform may believe the user had a good argument for non-infringement.[203]

Although some of the platforms themselves advocate for a DMCA-like safe harbor and process, they caution that it is not as simple as replacing the term "copyright" with "trademark."[204] Due to the differences between

200. Ramsey, *supra* note 190, at 455–56.

201. McGeveran, *supra* note 190, at 2303–2317 (arguing for safe harbors for titles of communicative works, news reporting and news commentary, and where trademarks are used in political speech).

202. *See* Etsy, et al., *supra* note 84, at 3. In fact, depending on the platform, trademark claims may outnumber the copyright-related ones. *See* ETSY, 2014 Transparency Report (Jul. 14, 2015), https://blog.etsy.com/news/files/2015/07/Etsy_TransparencyReport_2014.pdf.

203. *See* Etsy, et al., *supra* note 84, at 3 (discussing various examples of trademark uses that are abusive due to the likelihood that the user had a good non-infringement argument).

204. *Id.* at 5. Some commentators are also in favor of using the DMCA as a backdrop

the rights underlying copyright and trademark, we believe that a "notice and takedown" system is too blunt of an instrument, as it lacks the ability to take into account the nuanced analysis that is required of claims of trademark infringement.[205] For example, while copyright law provides for a relatively discrete examination of "substantial similarity," trademark law requires consideration of many more factors beyond similarity, including the marketing channels used, likelihood of "bridging the gap" between the goods of the defendant and the plaintiff, the defendant's intent, and evidence of actual confusion.[206] In the case of counterfeit merchandise, it becomes extremely difficult to tell whether the merchandise is actually fake or not.[207] And deferring to the plaintiff's determination opens up a host of potential problems that may facilitate abusive takedown requests, without independent examination.[208] Therefore, we suggest that the

for trademarks. *See* Elizabeth K. Levin, *A Safe Harbor for Trademark: Reevaluating Secondary Trademark Liability After* Tiffany v. eBay, 24 BERKELEY TECH. L.J. 491, 521–22 (2009) (arguing for a trademark statute that would parallel the DMCA). Other commentators argue for a somewhat modified system. For example, Frederick Mostert and Martin Schwimmer argue for an "expedited dispute resolution process" that combines the notice-and-takedown of the DMCA with due process akin to the current UDRP system. Frederick W. Mostert & Martin B. Schwimmer, *Notice and Takedown for Trademarks*, 101 TRADEMARK REP. 249, 271–80 (2011). It would appear, though, that many practitioners are in agreement with the ISPs that some type of solution is needed. Jason R. Brege & Kelli A. Ovies, *Taking Down Trademark Bullying: Sketching the Contours of a Trademark Notice and Takedown Statute*, 12 WAKE FOREST J. BUS. & INTELL. PROP. L. 391, 407 (2012).

205. Maayan Perel & Niva Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, 19 STAN. TECH. L. REV. 473 (2016). *See also* Teague, *supra* note 50, at 488–89.

206. Teague, *supra* note 50, at 489.

207. *Id.*

208. This has been seen in the copyright context. One study of the notices filed with Chilling Effects, renamed to Lumen (an online depository of DMCA notice-and-takedowns) noted a substantial number of notices from competitor to competitor, or from a big business to a blogger or hobbyist. *See* Jennifer M. Urban & Laura Quilter, *Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 651 (2006). More recent research led by Professor Urban sheds much-needed light into takedown practices. In part two of her three part, ground-breaking empirical research, Professor Urban shows that 70 percent of notices sent to social media sites contained questionable underlying legal claims. *See* Jennifer M. Urban, et al, *Takedown in Two Worlds: An Empirical Analysis*, 64 J. COPYRIGHT SOC'Y 483, 510 (2017). Although this high number includes problematic take-down notices from one particular individual, even without this individual's notices included in the sample, the percentage of problematic notices were approximately 36 percent. *See id.* For the full description of all three parts of Professor Urban's study, see Jennifer M. Urban, et al., *Notice and Takedown in*

United States needs to adopt a "notice and notice" framework, borrowing from Canada's recent adoption of such system in the copyright context.[209]

Unlike a notice and takedown format, which requires an ISP to take down the infringing content upon notice, a notice and notice framework would only require the ISP to forward the notice to the alleged infringer.[210] As one commentator argued, a notice-and-notice regime places the emphasis where it should be: on the alleged primary wrongdoer, and takes a more moderate approach to self-regulation by returning "intermediaries to their natural role as middlemen," restoring the responsibility to the courts for enforcement.[211] It also respects the privacy and expressive freedoms of end users more effectively than in a notice and takedown regime.[212]

In an ideal world, these notices from trademark owners would contain allegations of infringement for only those uses that were not within one of the categorical safe harbors as previously discussed. In such a world, then, compliance with the notice-and-notice framework would provide the ISP with immunity from secondary liability of its users' infringement. Even in a less-than-ideal world, compliance with the notice-and-notice framework provides more clarity surrounding procedures, even where the alleged infringements are not valid.

There are still some persistent questions, however. First, however, is the tricky question of who would qualify for the safe harbor and thereby should comply with a notice-and-notice regime. The DMCA, like the European Union E-Commerce Directive, categorizes ISPs into different types, depending on the service they provide. The DMCA's four categories are: (1) transitory digital network communications (the traditional service that ISPs provide, as in access to the internet for users);

Everyday Practice (University of California, Berkeley, Public Law Research, Working Paper), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628.

209. *See Notice and Notice Regime*, OFF. OF CONSUMER AFF. (Jan. 20, 2015), http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html.

210. Teague, *supra* note 50, at 488.

211. Christina Angelopoulous & Stijn Smet, *Notice-and-Fair-Balance: How to reach a Compromise Between Fundamental Rights in European Intermediary Liability,* 8 J. of Media L. 266, 295 (2016).

212. *Id.* It is worth noting that there is a difference in enforcement strategy between counterfeiting and trademark infringement due to the fact that counterfeiters will often simply ignore notices. The notice-and-notice proposal here does encompass these two different types of infringement, although recognizing that there are other approaches to handle pure counterfeiting. *See, e.g.*, Frederick Mostert & Marin Schwimmer, *Notice and Trackdown*, IP MAGAZINE, June 2011, at 18–19.

(2) system caching (this is where an ISP has made an automatic copy of a user's material in order to enable it to transmit); (3) information residing on systems or networks at direction of users (for example, where an ISP stores material on its system, but unlike in category (2), the storage is at the request of the user, and not an automatic technical process like caching); and (4) information location tools (this refers to services provided by search engines).[213]

While it would be handy to pull in these categories from the DMCA into our new framework, there would be a number of problems with such wholesale importation. First, due to the nature of trademarks and ISPs, an ISP's services could be categorized under more than one category.[214] For example, an e-commerce platform could fall into both the system caching, and potentially into the information location tool categories due to how they provide their retail services. This is problematic because for each category, the DMCA provides different conditions under which the ISP must follow in order to qualify for the immunity.[215] More concerning is that some categories, such as "information location tools" would be overbroad, as it does not distinguish between the different services that such ISPs offer, such as paid advertising services (like keyword ads) and organic services (where the ISP is simply indexing websites based on the natural searches and hits by users).[216]

One solution to these problems is to meld together the categories provided by the DMCA and by the EU E-Commerce Directive, as suggested by one commentator. Jordan Teague recommends that ISPs should be categorized according to how they interact with trademarks.[217] Teague identifies three different ways in which ISPs interact with trademarks: (a) where an ISP uses trademarks to identify products for sale (including directing users to similar products); (b) hosting content that contains trademarks; and (c) informational index trademark uses.[218] Teague then proposes that a trademark safe harbor framework would categorize ISPs into the following non-mutually exclusive types: "(1) information location tools; (2) advertising platforms; (3) online brokers;

213. 17 U.S.C. §512(a)–(d).

214. Teague, *supra* note 50, at 486.

215. For example, 512(d) requires information location tools to comply with the notice and takedown process, whereas 512(b) has a different set of requirements for system caching services.

216. Teague, *supra* note 50, at 486.

217. *Id.*

218. *Id.* at 486–487.

and (4) passive hosts."[219] This melds together the concepts from the DMCA and the EU E-Commerce, as it brings into the trademark context the recognition that ISPs are often actively interacting with trademarks (online brokers, advertising platforms) and sometimes they are passively storing the information (passive hosts).

With the categories identified, we can turn our attention to the procedures that would be undertaken by such ISPs in a notice-and-notice framework. As briefly outlined above, the trademark notice-and-notice system would be distinguished from the existing copyright notice-and-takedown one because the ISP would not be required to takedown any material. Upon receipt of the notice, the ISP would simply forward onto the user the notice it received from the trademark owner. It would be up to the user to takedown any material that was claimed to be infringing. Thus, the ISP would be immune from any secondary liability if it ended up that the user was in fact infringing another's trademark.[220]

While this sounds fairly straightforward, the lessons from Canada's implementation of the notice-and-notice regime for copyright infringement claims are helpful to heed. In particular, the potential for abuse needs to be carefully considered. Canada's legislation requires a number of items to be placed within the notice, but leaves it up to regulation as to specific language or template to be used.[221] Canada's Minister of Canadian Heritage and Official Languages decided to allow

219. *Id.* at 487.

220. Under the notice-and-takedown framework that is currently in place (and used for both copyright and trademark infringement claims), ISPs are required to act as the de facto judge to determine whether material is infringing or not. Due to the vague secondary liability standards, ISPs have stated that they err on the side of caution, oftentimes taking down material that they believe could have a plausible claim of non-infringement. *See* Etsy, et al., *supra* note 84, at 3–4. Another major shift in the notice-and-notice regime is that the ISPs would no longer need to serve as the de facto judge in the infringement analysis, with the hope of lowering error costs, as well as costs to the ISPs.

221. Canada Copyright Act, R.S.C. 1985, c-41.25(2) ("(2) A notice of claimed infringement shall be in writing in the form, if any, prescribed by regulation and shall(a) state the claimant's name and address and any other particulars prescribed by regulation that enable communication with the claimant; (b) identify the work or other subject-matter to which the claimed infringement relates; (c) state the claimant's interest or right with respect to the copyright in the work or other subject-matter; (d) specify the location data for the electronic location to which the claimed infringement relates; (e) specify the infringement that is claimed; (f) specify the date and time of the commission of the claimed infringement; and (g) contain any other information that may be prescribed by regulation.").

the implementation of the law without issuing any regulations.[222] In addition, the legislation provides that the ISP can face statutory damages of a minimum of CAN$5,000 (and up to $10,000) if they do not forward the notice to the alleged infringer.[223] The combination of these two items, a lack of regulation and a statutory damages award, has led to subscribers receiving abusive notices that claim they could be subject to a substantial fine (some notices claimed that the subscriber could face a $150,000 fine) and face suspension of their Internet accounts.[224] Both of these claims are false, as Canadian law limits the statutory damages award for non-commercial infringers to C$5,000 and there is no such provision regarding account suspension in the Canadian Copyright Act.[225] These abusive notices have led some subscribers to pay the fines, as well to an overall sense of confusion.[226]

Any notice-and-notice regime adopted in trademark law should likely include provisions regarding a form notice template with required language.[227] Serious thought needs to be given to drafting the form notice template that uses clear, non-legalese language, as well as governmental

222. Michael Geist, *Canada's Copyright Notice Fiasco: Why Industry Minister James Moore Bears Some Responsibility*, MICHAEL GEIST (Jan. 12, 2015) http://www.michaelgeist.ca/2015/01/canadas-copyright-notice-fiasco-industry-minister-james-moore-bears-responsibility/.

223. Canada Copyright Act, R.S.C. 1985 c-41.26(3). Although the law does not specifically state this, it could be reasonably assumed that the statutory damage award would be per instance. This would mean that for each notice that an ISP failed to forward, the ISP could face a statutory damage award of between $5000 and $10,000. This could quickly add up to an expensive proposition, as ISPs report that they have been receiving thousands of notices each day. *See* Claire Brownell, *Pirates in your neighbourhood: How new online copyright infringement laws are affecting Canadians one year later*, FP TECH DESK (Feb. 12, 2016 at 4:57 PM) http://business.financialpost.com/fp-tech-desk/pirates-in-your-neighbourhood-how-new-online-copyright-infringement-laws-are-affecting-canadians-one-year-later.

224. Michael Geist, *Canadians face barrage of misleading copyright demands*, TORONTO STAR (Jan. 9, 2015) https://www.thestar.com/business/tech_news/2015/01/09/canadians_face_barrage_of_misleading_copyright_demands.html.

225. *Id.*

226. Nicole Bogart, *No, you do not have to pay a 'settlement fee' if you get an illegal download notice*, GLOBAL NEWS (Jan. 13, 2017) http://globalnews.ca/news/3179760/no-you-do-not-have-to-pay-a-settlement-fee-if-you-get-an-illegal-download-notice/.

227. The ISPs in Canada are attempting to mitigate the lack of any required notice by including a "wrapper" that indicates to the user that the enclosed notice is merely an allegation of infringement, as well as directing the user to resources. Telephone Interview with Martin Simard, Director, Copyright and Trade-mark Policy Directorate (June 3, 2017) (notes on file with authors).

(or nonprofit) resources for the recipient of the notice to turn to with questions or concerns.[228] While the goal of a notice-and-notice system is to take the platform out of the role of enforcing trademark owners' rights, the pendulum should not swing so far to where users are left without any protections. As we can learn from the Canada example, it is likely that loopholes will exist in any legislation, even with well-thought out statutory language. Any notice-and-notice legislation should take this into account and build into the system a way in which regulations could be easily implemented to cover any unforeseen loophole that has a negative impact on users and the system as a whole.

We do note, however, that one of the major downsides to the above proposals in Section A and B is that we are calling for legislative action. And as seen in recent years, legislative changes, particularly where they do not ratchet up protection for trademark owners, will be difficult to get passed by the U.S. Congress. In addition, even if some of the proposed changes are taken under consideration by Congress, there is still a lengthy process before any changes would become effective. Some changes are needed in the short term. Therefore, this next subsection explores some common law changes that judges could undertake now through their interpretation of the Lanham Act and prior case law.

C. COMMON LAW CHANGES

Trademark scholarship and commentary is filled with suggestions as to how to reform trademark law in order to take into account the concerns facing trademark users.[229] The two suggestions we proffer here are (1) requiring a materiality of harm and (2) clarifying the duty to police. These two changes in the way judges approach trademark infringement cases can go a long way in mitigating some of the negative externalities that the

228. *See, e.g.,* Innovation, Science and Economic Development Canada, Office of Consumer Affairs, Notice and Notice Regime, Frequently Asked Questions, https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html (last visited on July 23, 2017).

229. For a small sampling of such work, s*ee generally* Graeme Dinwoodie, *Developing Defenses in Trademark Law*, 13 LEWIS & CLARK L. REV. 99 (2009) (arguing for courts to adopt stronger affirmative trademark defenses); Gerhardt, *supra* note 47 (suggesting a consideration of consumer investment in brands); Mark A. Lemley & Mark McKenna, *Irrelevant Confusion*, 62 STAN. L. REV. 413 (2010) (advocating that only source confusion should be presumed material in trademark litigation cases); Ramsey, *supra* note 190 (arguing that descriptive marks and slogans should be considered unconstitutional); Alexandra J. Roberts, *Tagmarks*, 105 CAL. L. REV. 599 (2017) (proposing a reconsideration of the registration of hashtags); Rebecca Tushnet, *Running the Gamut from A to B: Federal Trademark and False Advertising Law*, 159 U. PA. L. REV. 1305 (2011) (proposing a materiality standard for trademark law).

platform architecture, as it intersects with trademark law, produces.

1. Materiality of Harm Requirement

Trademark infringement doctrine is a species of tort law. The wrongful behavior is the infringement of a trademark. As with any tort, there needs to be an injury to the plaintiff that was caused by the defendant. In current trademark infringement cases, the injury caused by the defendant is the "likelihood of confusion" that the defendant's unauthorized use of their trademark could cause.[230] This "likelihood of confusion" analysis involves a multifactor test, which takes into account a number of different variables, such as the differences in the marketing channels of the plaintiff's and defendant's products, the type of product, etc.[231] Unlike other types of torts, missing from the analysis is an examination of whether defendant's use has, in fact, injured the plaintiff through a reduction in sales of plaintiff's products because there was actual confusion. Although actual confusion may be assessed as part of the multifactor test, it is not required for a fact finder to determine that a likelihood of confusion exists.[232] This is problematic because a defendant's guilt rests on speculation of what consumers would think and at no time is the plaintiff required to show what consumers have done in response to defendant's use.

Mark McKenna has argued that a presumption of harm is not warranted where a defendant's use of a mark is on goods that do not compete with the plaintiff's.[233] Additionally, Graeme Austin has argued that, "as a legal policy matter, equating trademark rights with what consumers might become confused about cannot be sufficient."[234] Rebecca Tushnet has long advocated for a return of a materiality element in trademark infringement cases, similar to that found in false advertising cases. She argues, "[r]egardless of what message consumers receive from the words and images in an ad, a far more important issue is what messages affect their decisions in identifiable ways."[235] This materiality

230. *See* Landes & Posner, *supra* note 44, at 302.

231. 4 J. THOMAS MCCARTHY, MCCARTHY TRADEMARKS AND UNFAIR COMPETITION § 23.19 (5th ed.).

232. *Id.*

233. Mark P. McKenna, *Testing Modern Trademark Law's Theory of Harm*, 95 IOWA L. REV. 63, 70–71 (2009).

234. Graeme W. Austin, *Tolerating Confusion about Confusion: Trademark Policies and Fair Use*, 50 ARIZ. L. REV. 157, 175 (2008).

235. Tushnet, *supra* note 229, at 1344.

would look at "whether consumers *care* whether a particular use of a trademark is made with the permission of the trademark owner. Often they do not."[236]

The practical implementation of this standard would be that the fact finders in a trademark infringement case would need to answer the question of whether a consumer would buy or perhaps pay more for a particular product based on a belief that the product was made by, or affiliated, sponsored, or endorsed by, the trademark owner.[237] If the answer is no, then the defendant's use of a mark that is either the same or similarly confusing to the plaintiff's is not material, and therefore, causing no harm. The case would be resolved in favor of the defendant. And this would still be true even if the defendant's use was likely to cause confusion.

The reintroduction of a materiality element would go a long way to rebalancing the relationship between the macrobrands and microbrands because a good deal of online trademark infringement claims deal with non-source-related confusion, such as sponsorship, affiliation or endorsement (such as in keyword advertising). In such cases, Mark Lemley and Mark McKenna advocate that where confusion is over the source of the product, there should be presumed materiality (although a rebuttable presumption), and other types of confusion should be presumptively immaterial.[238] This would strictly limit the types of actionable infringement claims that trademark owners could allege against microbrands in their notices to macrobrands, which could result in a more balanced relationship between the two. In the context of macro and microbrands in the platform ecosystem, this solution seems particularly appropriate to consider and employ.

2. Clarification of the "Duty to Police"

Although the Lanham Act does not explicitly require trademark owners to "police" their marks, over a half-century's worth of court cases does appear to place some type of burden on an owner to ward against infringing uses of their trademark.[239] The specifics of this duty, however,

236. *Id.* at 1366 (emphasis in original).

237. *Id.* at 1368.

238. Lemley & McKenna, *supra* note 229, at 445–46.

239. Jessica M. Kiser, *To Bully or Not to Bully: Understanding the Role of Uncertainty in Trademark Enforcement Decisions*, 37 COLUM. J.L. & ARTS 211, 224–26 (2014) (tracing the genesis of the duty to police).

remain unclear.[240] What is clear, though, is the *perception* by some trademark owners that this "duty" requires them to pursue possible infringers aggressively or else "lose their mark."[241] This perception is fueled by judicial statements such as this one from a 2003 Federal Circuit opinion, "Trademark law requires that the trademark owner police the quality of the goods to which the mark is applied, on pain of losing the mark entirely."[242] However, the actual loss of one's mark is extremely rare[243] and is therefore not a valid reason for over-enforcement.

The real driver for aggressive enforcement is the reward, as well as a lack of consequences for over-stepping the legal boundaries. Courts have taken as probative evidence aggressive enforcement strategies as proxies for a "strong" mark.[244] As one of us has argued in previous works, this aggressiveness can often cross the line into abusiveness where the parties in the dispute are imbalanced.[245] It is easy for a mark owner to slide into abusiveness, as trademark law lacks any mechanisms to hold trademark bullies accountable. There are virtually no consequences for over-enforcement.[246] But the rewards are great, as a strong or famous trademark is granted a larger scope of protection. Trademark owners whose marks are considered strong may bring infringement actions against defendants using the same or similar marks on unrelated products. In addition, owners of famous trademarks may bring dilution actions where defendants are using marks that can be associated with the famous mark, but is not even causing a likelihood of confusion. This enlarged scope of protection can provide some trademark owners with the ability to claim almost complete exclusivity over all uses of their marks. Given this lack of understanding

240. *Id.*

241. For example, the president of Monster Cable has been quoted as saying, "We have an obligation to protect our trademark; otherwise we'd lose it" as a rationale for the company's trademark bullying. Benny Evangelista, *Monster Fiercely Protects Its Name: Cable Products Company Sues Those Who Use M-Word*, S.F. GATE., Nov. 8, 2004, http://www.sfgate.com/bayarea/article/Monster-fiercely-protects-its-name-Cable-2675907.php. *See also* Jessica M. Kiser, *Brands as Copyright*, 61 VILL. L. REV. 45, 73 (2016) ("This duty to police serves as a justification for bully-like behavior by trademark owners"); Irina D. Manta, *Bearing Down on Trademark Bullies*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 853 (2012).

242. Nitro Leisure Prod., LLC v. Acushnet Co., 341 F.3d 1356, 1367 (Fed. Cir. 2003).

243. Kiser, *supra* note 241, at 73.

244. *See id*.

245. Grinvald, *supra* note 119, at 417–18.

246. *Id.*

of the duty to police one's trademark, the potential rewards, and the lack of consequences for over-enforcement, it is easy to understand aggressive (and perhaps even abusive) enforcement in the online space where uses of trademarks are ubiquitous.[247] Trademarks appear everywhere online, from blogs to reviews, to sales of used product listings.[248] An industry of "brand management" has arisen to help trademark owners police their trademarks online, which gives owners the ability to note any use of their mark.[249] Unfortunately, while not every use of a trademark is infringing, it may appear infringing to an over-zealous policer as long as it is unauthorized.[250] What this does is place trademark owners into overdrive in sending cease-and-desist letters or including trademark claims within take-down notices to platforms. As discussed above in Parts II and III, this places not only a serious burden on the platform, but risks unbalancing the ecosystem of the macrobrands and microbrands.

Related to this Article's suggested materiality requirement, but not mutually exclusive, is the proposal that judges make concerted efforts to clarify the "duty to police" one's trademark. A number of other commentators have previously noted this clarification is needed.[251] We agree with these commentators and further argue that what is needed are judicial pronouncements that would negate the effect of the Federal Circuit's 2003 statement as quoted above (and others like it).[252] Ideally,

247. In addition, Jessica Kiser's work in the emotional attachment to marks provides additional grounds to understand why trademark owners would want to be aggressive in their policing. *See generally* Kiser, *supra* note 241 at 73.

248. Eric Goldman, *Online Word of Mouth and its Implications for Trademark Law, in* TRADEMARK LAW & THEORY: A HANDBOOK OF CONTEMPORARY RESEARCH 411–12 (Dinwoodie & Janis eds., 2008); Deborah R. Gerhardt, *Social Media Amplify Consumer Investment in Trademarks*, 90 N.C. L. REV. 1491, 1524–26 (2012).

249. *See, e.g.*, CAPTERRA, Top Brand Management Software Products, http://www.capterra.com/brand-management-software/ (last visited Jun. 7, 2017) (listing 104 different brand management software).

250. *See* Kiser, *supra* note 241 at 73.

251. *See* Xiyin Tang, *Against Fair Use: The Case for a Genericness Defense in Expressive Trademark Uses*, 101 Iowa L. Rev. 2021, 2063 (2016); See Kiser, *supra* note 241, at 73.; Dogan, *supra* note 155, at 1319; Kenneth L. Port, *Trademark Extortion Revisited: A Response to Vogel and Schachter*, 14 CHI.-KENT J. INTELL. PROP. 217, 219 (2014); Jeremy N. Sheff, *Fear and Loathing in Trademark Enforcement*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 873, 877–79 (2012); Deven R. Desai & Sandra L. Rierson, *Confronting the Genericism Conundrum*, 28 CARDOZO L. REV. 1789, 1791, 1834–42 (2007).

252. Nitro Leisure Prod., LLC v. Acushnet Co., 341 F.3d 1356, 1367 (Fed. Cir. 2003).

there would be leadership on this issue from one of the circuits active in trademark law, such as the Second, Seventh, or Ninth Circuits. Consider, as an example, this pronouncement from Thomas McCarthy:

> The question is not how often or how assertively the trademark owner has enforced its mark, but what has been the marketplace loss of strength, if any, resulting from a failure to enforce. The real question is public perception of plaintiff's mark, not a battle count of how often it has threatened to sue or in fact sued.[253]

As to McCarthy's argument that it is the public perception that matters in these cases, courts must stop rewarding bad behavior. Instead of accepting the fallacy that a lack of third party use automatically equates to high levels of trademark strength or fame, as some trademark owners argue, courts should require stronger evidence of such acquired distinctiveness. Although surveys are notoriously problematic,[254] courts should require plaintiffs who argue strength or fame to conduct a consumer survey of how consumers view their trademark. Currently surveys are not required, although there are indications that some judges expect surveys, particularly from large trademark owners.[255] A consistent application of this heightened level of evidence for claims of strength or fame could go a long way in lowering the expectations of some trademark owners for their "reward" in over-policing their marks.

***

Of course, the downside to relying on judges as vehicles of change is that it is haphazard, as judicial change is reliant on good cases being brought before a judge so inclined to interpret the Lanham Act and prior case law the way we (and others) suggest that it could be interpreted. However, incremental change does have an effect, and one influential case can have enormous ripple effects, as we saw with the Second Circuit's *eBay* case.

Another downside is that, as we have noted above, a good portion of all trademark-related disputes occur outside of a courtroom and so there will be many instances where the law does not directly reach. However, as William Gallagher has shown in his qualitative empirical study of

253. 4 J. THOMAS MCCARTHY, MCCARTHY TRADEMARKS AND UNFAIR COMPETITION § 11:91 (5th ed.).

254. *See id.* § 15:42.

255. *See id.* § 32:195.

intellectual property lawyers, these informal disputes are settled in the "shadow of the law."[256] Therefore, even a handful of good cases that apply a materiality of harm requirement or clarify what it means to adequately police one's trademark will be helpful in guiding lawyers as they assist their clients. Ideally these "good" cases would feed into lawyers' advice to their clients to *not* bring claims of infringement that rest on trademark uses outside the realm of core trademark concerns (i.e., source confusion).

V. CONCLUSION

As suggested throughout this Article, at the same time that the absence of law has facilitated the rise of platforms, there is now a growing need for sophisticated legal systems to sustain the possibilities for platform innovation and protection. This is particularly true of trademark law, where the platform has both challenged established theories of contributory liability at the same time that it has facilitated the need for increased regulation.

This Article has argued that trademarks play a particular role in the design and formation of nearly every aspect of a platform, producing two central formations: macrobrands and microbrands. In turn, the formation of these two systems, and the intersection between them, both challenge and transform trademark law as a result, opening up new questions and opportunities. In order to protect the vitality and innovation of the platform ecosystem, trademark law must begin to reinvent itself in addressing contributory liability. Rather than turning to copyright law and the DMCA as an example of how to govern online infringement, this Article instead argues for the employment of additional tools – a notice and notice system, in particular – in order to restore intermediaries to their original roles and limit the significant administrative costs associated with enforcement. By considering both legislative reform and common law adjustments, trademark law can facilitate an even greater level of growth and innovation within the platform ecosystem.

256. William T. Gallagher, *Trademark and Copyright Enforcement in the Shadow of IP Law*, 28 SANTA CLARA COMPUTER & HIGH TECH. L. J. 453, 456 (2011).

DESIGNING AGAINST DISCRIMINATION IN ONLINE MARKETS

Karen Levy[†] *& Solon Barocas*[††]

ABSTRACT

Platforms that connect users to one another have flourished online in domains as diverse as transportation, employment, dating, and housing. When users interact on these platforms, their behavior may be influenced by preexisting biases, including tendencies to discriminate along the lines of race, gender, and other protected characteristics. In aggregate, such user behavior may result in systematic inequities in the treatment of different groups. While there is uncertainty about whether platforms bear legal liability for the discriminatory conduct of their users, platforms necessarily exercise a great deal of control over how users' encounters are structured—including who is matched with whom for various forms of exchange, what information users have about one another during their interactions, and how indicators of reliability and reputation are made salient, among many other features. Platforms cannot divest themselves of this power; even choices made without explicit regard for discrimination can affect how vulnerable users are to bias. This Article analyzes ten categories of design and policy choices through which platforms may make themselves more or less conducive to discrimination by users. In so doing, it offers a comprehensive account of the complex ways platforms' design and policy choices might perpetuate, exacerbate, or alleviate discrimination in the contemporary economy.

DOI: https://doi.org/10.15779/Z38BV79V7K

† Assistant Professor of Information Science, Cornell University; Associated Faculty, Cornell Law School.

†† Assistant Professor of Information Science, Cornell University. We are immensely grateful to our team of research assistants—Jevan Hutson, Jessie Taft, and Olivia Wherry—for their stellar assistance with both data collection and synthesis. In addition, we thank Matt Cagle, Anna Lauren Hoffmann, Amy Krosch, Nicole Ozer, David Pedulla, and participants in the 21st Annual BCLT/BTLJ Symposium, Platform Law: Public and Private Regulation of Online Platforms, for helpful feedback.

TABLE OF CONTENTS

Web-based platforms frequently make a range of socially salient characteristics available to transacting parties. Names and photos, for example, are a standard feature of user profiles on platforms that aim to connect buyers and sellers, hosts and guests, drivers and riders, and all manner of online daters. Such details have a long-standing place on platforms as mechanisms to establish trust between strangers transacting online.

Design features like these have allowed platforms that function as online marketplaces to flourish. The early web was marked by considerable uncertainty as to the reliability of the person on the other side of some exchange. Today's web is dominated by platforms that employ a diverse set of techniques to relieve users of such anxieties—providing assurances that can go far beyond what people might glean from in-person interactions.

In adopting these techniques, however, platforms have begun to exhibit the sorts of worrisome dynamics that are common in face-to-face encounters. Platforms that highlight users' socially salient characteristics invite users to take these characteristics into account, even when they might not—or should not—be relevant to the interactions facilitated by the platform. Names and photos, for example, can reveal users' gender, race,

ethnicity, national origin, religion, age, or disability, among other details. Such details have allowed users to discriminate against one another—either by conscious choice or unconsciously due to implicit bias. When these details are made more prominent, more readily available, or simply unavoidable, they can affect users' behavior in ways that correspond to established patterns of bias in offline markets: users may refuse to transact, make less attractive offers, or evaluate each other less favorably.

When a customer enters a store, a job applicant submits a resume, a passenger flags down a cab, a potential tenant visits a property, or a person strikes up a conversation at a singles bar, the person cannot help but reveal characteristics that might lead to biased impressions. In contrast, online platforms have far more control over how these encounters are structured.[1] Platforms mediate interactions in ways that can both mitigate and aggravate bias. Design and policy choices make platforms more or less conducive to discrimination in user-to-user interactions. Platforms cannot divest themselves of this power; even choices made without explicit regard for discrimination can affect how vulnerable users are to bias. This is true even when pursuing other laudable goals like attempting to ensure greater trust, smoother interactions, or a more efficient market among users.

At the same time, platforms can *purposefully* attempt to address the role of bias in users' exchanges—for instance, by stripping interactions of obvious visual or verbal cues, allowing users to transact in relative anonymity. Ride-hailing services, like Uber and Lyft, have touted features of their platforms that make it difficult or impossible for drivers to discriminate when choosing whether to make a pick-up. Drivers do not learn the identity or intended destination of riders until drivers accept a request.[2] Platforms can decide what information passes through their channels and thus limit the flow of information upon which discrimination depends.

---

1. Ray Fisman & Michael Luca, *Fixing Discrimination in Online Marketplaces*, HARV. BUS. REV., Dec. 2016, at 88.

2. Johana Bhuiyan, *Uber and Lyft Position Themselves as Relief from Discrimination*, BUZZFEED (Oct. 7, 2014, 11:05 AM), https://www.buzzfeed.com/johanabhuiyan/app-based-car-services-may-reduce-discrimination-issues-tk. Note that Lyft shows drivers the names and photos of passengers once drivers accept riders' request, which allows Lyft drivers to then cancel the rides once they have learned about passengers. However, Lyft passengers are not required to upload photos, so this dynamic only applies when passengers have volunteered photos of themselves. In contrast, Uber never shows photos to drivers. Eric Newcomer, *Study Finds Racial Discrimination by Uber and Lyft Drivers*, BLOOMBERG (Oct. 31, 2016, 10:51 AM), https://www.bloomberg.com/news/articles/2016-10-31/study-finds-racial-discrimination-by-uber-and-lyft-drivers.

But platforms' role in modulating the extent to which users might discriminate against one another extends well beyond deciding what users can learn about each other. Platforms also decide *how* users learn about each other: users might receive recommendations, perform searches, or filter according to fixed criteria. Some platforms decide *who* can join these online communities, conditioning entry on various facets of users' offline identities. And many decide to adopt mechanisms that allow users to rate and comment upon one another for others to see—the basis of reputation systems that are ubiquitous online. These choices structure users' encounters and interactions in particular ways, even when platforms see themselves as nothing more than passive conduits through which users engage with one another.[3] Platforms that mediate between users necessarily moderate how users behave on these platforms, including how easily users can fall victim to their implicit biases or how effectively they can impose their prejudicial beliefs on others. Platforms are thus in a privileged and difficult position. The *ability* to mediate interactions between users may create a perceived *responsibility* to do so—even if a platform does not bear legal liability for users' biased behavior.

Platforms that recognize the influence they wield over their users—including platforms that have been pressured to acknowledge such influence—tend to rely on a diverse set of mechanisms to minimize the degree to which users can engage in discriminatory conduct: company initiatives that aim to increase sensitivity to issues of discrimination by cultivating greater workplace diversity and fostering inclusion; the development, adoption, and championing of community policies that forbid or repudiate any discrimination on the part of users; direct attempts to intervene in the process by which users' prejudices or implicit biases enter into their decision-making, involving prompts and priming; the use of additional sources of data to validate users' claims; or introducing systems for users to report instances of discrimination and impose corresponding sanctions. Some have even begun to track disparities in users' experiences on the platform, according to their race, gender, or other protected characteristics, and to identify specific cases of prejudicial or biased decision-making.

Platforms' role in mediating users' discriminatory behavior is complicated by the currently unresolved application of law in this area. Numerous user-to-user platforms operate in domains traditionally within

3. *See* Tarleton Gillespie, *The Politics of 'Platforms'*, 12 NEW MEDIA & SOC'Y 347, 352–353 (2010).

the reach of antidiscrimination law, like housing and employment.[4] Within these domains, however, the applicability of anti-discrimination law to platforms—and specifically to users' interactions among themselves *as mediated by* platforms—is unsettled. Despite their immense power to shape a wide variety of interactions integral to social and economic life, platforms' business models have enabled them to largely sidestep the traditional regimes that protect against discrimination and other harms in those interactions.[5] Platforms routinely disclaim legal responsibility for all kinds of harms propagated by their users against one another,[6] and have largely been successful in so doing.

Despite this, recent calls aim to extend liability to platforms for underlying user conduct within subject domains where existing civil rights law prohibits discrimination. Notably, Belzer and Leong argue that public accommodation laws (including Title II of the Civil Rights Act of 1964 and the Fair Housing Act) must be newly interpreted to remedy discrimination that occurs *between users* on "sharing economy" platforms, considering these platforms' functional equivalence to the types of establishments to which those laws have traditionally applied (hotels, taxi services, and the like).[7]

Even if antidiscrimination law can be viably extended to platforms for users' discriminatory conduct, platforms often assert immunity based specifically on their status as platforms. Section 230 of the Communications Decency Act immunizes a provider of "an interactive computer service" from being treated as the publisher of information provided by its users[8]—

4. Other platforms operate in domains to which federal antidiscrimination law is less obviously applicable. On these platforms, where law may not provide a ready remedy for users' behaviors that might systematically disadvantage certain groups, design interventions may be even more important tools for the mitigation of bias.

5. *See generally* Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87 (2016). Some of this is due to platforms' poor fit with traditional models of employment—for instance, their tendency to take steps to ensure that service providers are not characterized as employees of the platform company. *See* Alex Rosenblat et al., *Discriminating Tastes: Uber's Customer Ratings as Vehicles for Workplace Discrimination*, 9 POL'Y & INTERNET 256, 266-67 (2017).

6. *See, e.g.,* Talia G. Loucks, *Travelers Beware: Tort Liability in the Sharing Economy*, 10 WASH. J.L. TECH. & ARTS 329, 335, 338 (2015).

7. *See* Aaron Belzer & Nancy Leong, *The New Public Accommodations*, 105 GEO. L. J. 1271, 1271 (2017). *See also* Michael Todisco, *Share and Share Alike? Considering Racial Discrimination in the Nascent Room-Sharing Economy*, 67 STAN. L. REV. ONLINE 121, 128–29 (2015); Katharine T. Bartlett & Mitu Gulati, *Discrimination by Customers*, 102 IOWA L. REV. 223, 249–50 (2017).

8. 47 U.S.C. § 230(c)(1).

including, often, information and conduct that exhibits bias.[9] CDA 230 has proved the most important tool upon which platforms currently rely to avoid liability for their users' conduct. Though the applicability of the statute has not yet been thoroughly tested with respect to the platform economy,[10] courts have sometimes seen fit not to apply immunity when platforms' actions "help[] to *develop* [users'] unlawful content"[11] through how such information is solicited or structured on the site. In the most prominent case in which a court so found, *Fair Housing Council of San Fernando Valley v. Roommates.com*,[12] the Ninth Circuit held that Roommates.com (a listing service for prospective roommates seeking housing, and vice versa) was not entitled to CDA 230 immunity because its site had featured dropdown menus through which users were required to provide information about their gender and sexual orientation, as well as their preferences about the corresponding characteristics desired in a roommate. In structuring users' interactions in such a way, the Court found that the platform had "[made] answering the discriminatory questions a condition of doing business."[13]

Roommates brought platform design to the fore as a potentially determinative factor in resolving whether platforms are immune from discrimination claims based on user conduct. The case has generated a significant amount of legal scholarship, focused primarily on issues related to how the case augurs for the future contours of the CDA's immunity protection.[14] But less attention has been paid to the first-order question of what sorts of design decisions platforms make that might mitigate or

9. *See, e.g.*, Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008). In *Craigslist*, the Seventh Circuit ruled that Craigslist was entitled to CDA 230 immunity for user posts containing discriminatory housing limitations (such as "NO MINORITIES"). In so ruling, the court noted that Craigslist had merely "provid[ed] a place where people can post" housing ads, and that "[n]othing in the service [C]raigslist offers induces anyone to post any particular listing or express a preference for discrimination." *Id.* at 671.

10. Belzer & Leong, *supra* note 7, at 1320–21.

11. *Fair Housing Council of San Fernando Valley v. Roommates.com*, 521 F.3d 1157, 1168 (9th Cir. 2008) (emphasis added).

12. *Id.*

13. *Id.* at 1181. Similarly, the Court also found that the platform's search and filter system was not entitled to CDA immunity, as the platform "designed its search system so it would steer users based on the preferences and personal characteristics that Roommate itself forces subscribers to disclose. … [Roommates.com] designed its system to use allegedly unlawful criteria so as to limit the results of each search, and to force users to participate in its discriminatory process." *Id.* at 1167.

14. *See, e.g.,* Belzer & Leong, *supra* note 7; Varty Defterderian, *Fair Housing Council v. Roommates.com: A New Path for Section 230 Immunity*, 24 BERKELEY TECH. L.J. 563 (2009); Bradley M. Smyer, *Interactive Computer Service Liability for User-Generated Content After Roommates.Com,* 43 U. MICH. J. L. 811 (2010).

exacerbate the role of users' biases. This Article's focus, then, is not to explore the potential applicability of antidiscrimination statutes or CDA immunity to platforms; rather, it is to complement and expand those areas of active scholarly discussion with empirical exploration of platforms' design and policy choices.[15]

This Article provides a conceptual framework for understanding how platforms' design and policy choices introduce opportunities for users' biases to affect how they treat one another. We do so through empirical review of design-oriented interventions used by a range of platforms and the synthesis of this review into a taxonomy of thematic categories. In so doing, we hope to prompt greater reflection on the stakes of such decisions as they are made by platforms already, guide platforms' future decisions, and provide a basis for empirical work measuring the impacts of design decisions on discriminatory outcomes.

We proceed as follows. In Part I, we describe our empirical review of platforms, and the strategies we used to develop our taxonomy. In Part II, we present in detail the ten thematic categories that emerged from this review and describe how platforms' design interventions might mediate or exacerbate users' biased behaviors, drawing from social and psychological research on bias and stereotyping. Further, we discuss the interactions among design features, and the importance of acknowledging these interactions to effectively address bias. Part III describes the ethical dimensions of platforms' design choices—including when platforms might *not* want to attempt to mitigate users' biases—and concludes.

I. METHODS

Our analysis is based on a review of over fifty platforms spanning several domains. We specifically set out to identify platforms in the following seven areas, where online platforms have assumed an important role: consumer-to-consumer sales; transportation; tasks and gigs; hiring; housing; crowdfunding and lending; and dating. We identified the dominant platforms in each area. We also included widely recognized companies in

15. Notably, legal proceedings (or the specter thereof) have had the effect of requiring platform companies to address user-to-user bias through design alterations. As described *infra*, the voluntary agreement between Airbnb and the California Department of Fair Employment and Housing (in resolution of the lawsuit filed by the agency against Airbnb) mandates that Airbnb adopt, or consider adopting, a number of design-relevant strategies in order to reduce discrimination. Hence, platform design choices can intersect intimately with anti-discrimination law, both by moderating avenues to liability and by serving as a means to resolve litigation.

our survey, particularly those that have received attention in existing scholarship and media coverage on the problem of bias in users' interactions. Finally, we attempted to identify platforms that have made public statements committing to address bias.

We then explored the user experience on each of these platforms, systematically documenting design choices that created or limited opportunities for users to purposefully discriminate against one another or for users' implicit biases to influence their behaviors. Our initial efforts were informed by existing research on how design decisions can assist in successfully constructing and regulating online communities,[16] particularly dealing with troubling user behavior (e.g., trolling and harassment).[17] We examined how users experience these platforms when connecting via the web or apps; of the platforms we examined, the majority exist as mobile-only apps. In both cases, we created user accounts on each platform, as most do not allow non-users to access even basic features or functionality. We reviewed how a typical user might interact with the website or app. Our review paid particular attention to features that had been the focus of previous research, notably the contents of user profiles and product listings, all manner of sorting and rating mechanisms, the presence or absence of terms of service, community guidelines, or any explicit statements about bias or discrimination, as well as tools to report unsanctioned user behavior.

For ethical reasons, we limited our exploration to situations where we could observe or make use of a feature without directly interacting with other users. We reasoned that engaging users in transactions that we did not intend to complete, for example, would be dishonest and would waste the time of the other user. Sometimes, we were unable to document features only available to users during or after their interactions with others. We also refrained from taking any action that could potentially cause harm or negative outcomes for other users. For example, in many cases, platforms offer the opportunity to report or flag other users or content (as we describe in Part II.C.1, *infra*). To avoid reporting innocent users, we refrained from clicking on "Report" links unless it was obvious that the link would lead to a list of options (which we would not complete) and would not immediately report the user or content. In cases where some information about the platform was inaccessible, we made attempts to find relevant details by

16. *See, generally,* Robert E. Kraut et al., BUILDING SUCCESSFUL ONLINE COMMUNITIES: EVIDENCE-BASED SOCIAL DESIGN (2012). Kraut et al.'s framework of design strategies for online communities consists of eight design categories that can govern how users are allowed to behave in their interactions.

17. J. Nathan Matias et al., *Online Harassment Resource Guide*, WIKIMEDIA (July 3, 2015), https://meta.wikimedia.org/wiki/Research:Online_harassment_resource_guide.

other means. This often meant locating the platform's how-to guides, which walk new users through the process of interacting or transacting with others and often include images of the platform's interface at each stage in the process.

In reviewing the features of each platform, we found commonalities across various design and policy choices and grouped these into ten categories described below and summarized in the following table. These categories cluster into three general groups: setting platform- and community-wide policies, structuring users' encounters and experiences on the platform, and monitoring and evaluating platform activity to root out bias. Our taxonomy of design choices is not intended as an endorsement of any particular strategy for dealing with bias, nor as an empirical assessment of the efficacy of these interventions. Instead, this Article aims to provide the first comprehensive and coherent account of the many ways that platforms can—and often already—attempt to limit discrimination between users.

Table 1: Overview of platform policy and design strategies

Strategy		Examples
Setting policies	Company-level diversity and anti-bias strategies	Increasing diversity within the company workforce; educating employees about bias; engaging underrepresented groups in the design process
	Community composition	Restricting community through norms, rules, and structures
	Community policies and messaging	Community guidelines; required training on community norms; pledges; language and imagery on- and off-site
Structuring interactions	Prompting and priming	Prompting user to reflect on their behavior at specific decision points
	How users learn about one another	Matching users; searching; filtering
	What users learn about one another	Encouraging or requiring disclosure of user information; withholding user information; structuring the presentation of user information
	Reputation, reliability, ratings	Testimonials; references; reviews; badges; ratings
Monitoring and evaluating	Reporting and sanctioning	Creating mechanisms for user to report biased behavior; sanctioning users who discriminate
	Data quality and validation	Requiring more granular information; adjusting ratings; delisting reviews; requiring validation from external data
	Measurement and detection	Collecting demographic data to measure disparities in outcome by protected characteristics; experimenting with design to assess effects on bias; opening data to outside scrutiny

II. HOW PLATFORMS MEDIATE BIAS IN USER-TO-USER INTERACTIONS

A. SETTING POLICIES

Platforms' corporate and community-wide policies may affect the degree to which discrimination occurs among users. A focus on diversity and inclusion in corporate teams and the design process can sensitize the platform to bias-related issues. Defining and limiting the community along specific lines can help to establish greater affinity among users, thereby reducing the likelihood that users will rely on biased heuristics when engaging with others. Finally, creating and communicating rules and norms for users' conduct can be a way to discourage and sanction biased behavior.

1. Company-level diversity and anti-bias strategies

To address issues of systemic bias on platforms, some companies have adopted strategies that aim to address the problem by reforming the company *itself*. Companies might seek to address platforms' role in mitigating bias *from within*, by altering their own organizational makeup, internal policies, and design processes. For example, platform companies may seek to increase the representation of underrepresented groups within their engineering teams through targeted hiring initiatives or strategies aimed at mitigating bias and discrimination in internal hiring processes. Companies may offer specialized training to their engineering teams and other members of their workforce about implicit bias and its effects, or firms may devote particular personnel and other internal resources to the project of bias elimination. Finally, firms may explicitly integrate engagement with underrepresented groups in their design processes.

Airbnb employed each of these approaches as part of the reforms associated with its 2016 nondiscrimination review, conducted in response to findings of systemically worse outcomes for black users seeking short-term housing on the site.[18] It sought to increase diversity in its workforce by implementing a "Diversity Rule" requiring that all candidate pools for senior positions include underrepresented minorities and women,[19] premised on the idea that the company "may have been slow to address concerns about discrimination because [its] employees are not sufficiently

18. Laura W. Murphy, Airbnb's Work to Fight Discrimination and Build Inclusion 22, 24 (Sep. 8, 2016), http://blog.atairbnb.com/wp-content/uploads/2016/09/REPORT_Airbnbs-Work-to-Fight-Discrimination-and-Build-Inclusion.pdf.

19. *See id*. at 12.

diverse."[20] In addition, Airbnb increased recruitment efforts for underrepresented groups, and included a diversity measure in the assessment of hiring managers.[21] It expanded and required anti-bias training for all its employees, with specialized training for customer service representatives who interact directly with hosts,[22] and created a new team of engineers, designers, data scientists, and researchers devoted to anti-bias projects.[23] Airbnb's review was developed in consultation with a range of end users, as well as representatives from a number of civil rights and advocacy organizations.[24]

Some strategies in this category assume a sort of "trickle-down" approach to bias mitigation. The presence of more diverse company personnel (perhaps especially engineers) and explicit training about the problem of implicit bias may attune companies to the potentially disparate effects of their design decisions that might not have come to the fore otherwise.[25] Internal strategies such as targeted hiring or company-wide

20. *Id.* at 17. This policy—commonly known as the "Rooney Rule," after Pittsburgh Steelers chairman Dan Rooney, who implemented a similar approach in the National Football League—has recently gained traction in Silicon Valley in response to calls for greater diversity in tech employment. Davey Alba, *The NFL is Showing Silicon Valley How to Be More Diverse*, WIRED (Oct. 26, 2015), https://www.wired.com/2015/10/tech-silicon-valley-nfl-rooney-rule-diversity/ (describing tech companies' increasing adoption of the Rooney Rule to increase diversity in management roles).

21. Murphy, *supra* note 18, at 24 (noting that Airbnb planned to increase the proportion of underrepresented minorities in its U.S. workforce from 9.64% in September 2016 to 11% by the end of 2017).
Id. at 22.

23. *Id.* at 24.

24. *Id.* at 15; *see* Jessi Hempel, *For Nextdoor, Eliminating Racism is No Quick Fix*, BACKCHANNEL (Feb. 16, 2017, 12:00 AM), https://backchannel.com/for-nextdoor-eliminating-racism-is-no-quick-fix-9305744f9c6 (describing Nextdoor's consultation with racial justice groups and government officials in their efforts to mitigate user bias on the platform, in which they "began holding regular working groups in which they included these people in the product development process"). These approaches relate to participatory design processes, through which designers consult with and integrate stakeholders throughout the design process in order to address needs and concerns of users that might not otherwise be apparent. *See* Christopher A. Le Dantec & Carl DiSalvo, *Infrastructuring and the Formation of Publics in Participatory Design*, 43 SOC. STUD. SCI. 241 (2013).

25. Similarly, measures to increase within-company diversity have been espoused in response to other instantiations of bias on platforms and in algorithms. *Cf.* Kate Crawford, *Artificial Intelligence's White Guy Problem*, N.Y. TIMES, Jun. 26, 2016, at SR11 (relating lack of corporate inclusivity to bias in artificial intelligence); Charlie Warzel, *"A Honeypot for Assholes": Inside Twitter's 10-Year Failure to Stop Harassment*, BUZZFEED (Aug. 11, 2016), https://www.buzzfeed.com/charliewarzel/a-honeypot-for-assholes-inside-twitters-10-year-failure-to-s (relating Twitter's leadership homogeneity and corporate culture to its difficulties in stemming abuse and harassment for users).

training may also appeal to, and dovetail with, other corporate goals about diversity and inclusion, particularly given recent efforts to address the vast underrepresentation of women and minorities in Silicon Valley and the exclusionary corporate cultures at tech firms.[26]

However, diversity and inclusion measures are unlikely to themselves be a panacea for addressing bias in hiring and corporate culture—not to mention for influencing platform design choices that may facilitate user-to-user bias. The efficacy of unconscious bias and diversity training has not been established empirically.[27] In some cases, such trainings may even *exacerbate* biased behavior by normalizing biased attitudes (e.g., by suggesting that "everyone is biased")[28] or by causing people to retaliate against feelings of pressure, social judgment, and control.[29]

2. Community composition

A second set of strategies involves creating barriers to membership in a platform-mediated community by implementing rules or expectations about the characteristics members must meet in order to participate on the platform. Such restrictions may be based on membership in a demographic category (e.g., JDate,[30] a dating website for Jewish users), geographic proximity (e.g., neighborhood sites on Nextdoor[31]), shared professions or interests (e.g., FarmersOnly,[32] for farmers, and VeggieDate,[33] for vegetarians), or other limitations.

---

26. *See, e.g.,* Liza Mundy, *Why is Silicon Valley So Awful to Women?* THE ATLANTIC (April 2017), https://www.theatlantic.com/magazine/archive/2017/04/why-is-silicon-valley-so-awful-to-women/517788/ (describing how "unconscious-bias training has emerged as a ubiquitous fix for Silicon Valley's diversity deficit").

27. *See generally* Elizabeth Levy Paluck & Donald P. Green, *Prejudice Reduction: What Works? A Review and Assessment of Research and Practice,* 60 ANN. REV. PSYCH. 339 (2009); Frank Dobbin & Alexandra Kalev, *Why Diversity Programs Fail*, HARV. BUS. REV., Jul. 2016 at 52.

28. *See* Michelle M. Duguid & Melissa C. Thomas-Hunt, *Condoning Stereotyping? How Awareness of Stereotyping Prevalence Impacts Expression of Stereotypes*, 100 J. APPLIED PSYCHOL. 343, 354 (2015) (suggesting that increasing awareness of stereotyping can normalize prevalent stereotypes). *See also* Jessica Nordell, *Is This How Discrimination Ends?*, THE ATLANTIC (May 7, 2017), https://www.theatlantic.com/science/archive/2017/05/unconscious-bias-training/525405/ (detailing strengths and weaknesses of the widely used Implicit Association Test ("IAT") and various anti-prejudice interventions).

29. Lisa Legault et al., *Ironic Effects of Antiprejudice Messages: How Motivational Interventions Can Reduce (but Also Increase) Prejudice,* 22 PSYCHOL. SCI. 1472 (2011).

30. JDATE, https://www.jdate.com (last visited July 15, 2017).

31. NEXTDOOR, https://nextdoor.com (last visited July 15, 2017).

32. FARMERSONLY, https://www.farmersonly.com (last visited July 15, 2017).

33. VEGGIEDATE, http://www.veggiedate.org (last visited July 15, 2017).

Community composition can be limited by a platform in a number of ways. The simplest mechanism is for the platform to establish that the community is *for* some users—and, concomitantly, *not* others—through messaging. JDate, for example, does not police whether its members are in fact Jewish, but indicates that the site is intended for Jewish users through its site text, logo, and other elements.[34] The operative assumption seems to be that this norm and purpose will be enforced through self-selection into the community of users.

Other sites enforce community composition norms more structurally—for instance, by requiring users to possess a credential, like an email address from a prescribed domain or set of domains. In its early days, Facebook was restricted only to users with .edu email addresses from select colleges and universities.[35] Other sites' user bases are restricted based on network proximity (for instance, new users must be within *x* degrees of existing users in an articulated social network, like LinkedIn or Facebook), or allow new users in when invited by existing members. Nextdoor, for example, requires prospective users to verify their home addresses before gaining access to the site. It offers several options for doing this, including providing social security or credit card information linked to the address. Alternatively, prospective users can skip the verification process by receiving invitation codes from already-verified neighbors.[36] The civic engagement platform PlaceSpeak (which provides a venue for residents of an area to comment on local issues) allows users to authenticate themselves via several methods, including "linking to social media profiles, verifying IP addresses, and confirming identities over the phone"[37]; further, the more heavily authenticated a user is, the more her input is weighted in the discussion.[38]

34. JDate addresses the possibility that non-Jewish users might sign up for the site. *See* About JDate, Who Uses JDate?, https://www.jdate.com/help/about/(noting "JDate is designed for Jewish singles of all ages looking to connect based on common ground. That being said, JDate is open to all singles 18 years or older. If you're not Jewish and you're still interested in joining JDate, please ensure that the religion section of your profile indicates whether or not you are willing to convert").

35. Sarah Phillips, *A Brief History of Facebook*, THE GUARDIAN (Jul. 25, 2007), https://www.theguardian.com/technology/2007/jul/25/media.newmedia.

36. Getting Started, NEXTDOOR, (Jun. 20, 2017), https://help.nextdoor.com/customer/en/portal/articles/805357-verify-your-address.

37. Zack Quaintance, *New Resident-Facing Platform Seeks Public Input, Minus the Trolls*, GOVTECH (Jun. 30, 2017), http://www.govtech.com/civic/New-Resident-Facing-Platform-Seeks-Public-Input-Minus-Trolls.html.

38. *Id.* In this way, user authentication is treated as a proxy for data quality. *See infra* Part II.C.2.

Finally, platforms may police membership through independent vetting. Uber screens potential drivers by requiring a background check, which it contracts out to a third-party company; that company screens the potential driver for criminal history, suspected terrorist activity, presence on the National Sex Offender Registry, and other information.[39] Airbnb and Uber are reportedly considering using Aadhaar, India's controversial biometric identity database, to validate users' identities.[40] However, logistical concerns—such as the expense of background checks, the time required to complete them, and diverse regulatory environments—may limit the use of such tools on other platforms.[41]

Restricting access to a community—through norms, rules, or structures—may, of course, be a relatively overt way for a platform to *itself* propagate bias through explicit exclusion of particular groups from participation (and, concomitantly, from the social and economic opportunities that such participation might afford). But, in addition, measures that restrict community composition may exacerbate or mitigate bias in interactions *between users* on platforms.

In some cases, restricting access may help to cultivate a baseline level of affinity, homogeneity, connection, or trust among users that may militate against bias in their interactions. In particular, users may refrain from reliance on stereotypes about *secondary* characteristics because negative associations based on those characteristics are neutralized by membership on the platform—and the associated characteristics it imparts. Users who perceive themselves to be similar along some dimension, who are prone to repeated interaction (based, for instance, on geographic proximity), or who are inclined to trust one another because of external vetting or credentialing may be less likely to fall back on biases about other characteristics[42]: for

39. Sarah Kessler, *The Truth About Uber's Background Checks*, FAST COMPANY (Aug. 26, 2015), https://www.fastcompany.com/3050172/the-truth-about-ubers-background-checks. Uber has been criticized for the thoroughness of its background checks; *see* Adrienne LaFrance & Rose Eveleth, *Are Taxis Safer than Uber?*, THE ATLANTIC (Mar. 3, 2015), https://www.theatlantic.com/technology/archive/2015/03/are-taxis-safer-than-uber/386207/.

40. Pranav Dixit, *Airbnb, Uber, and Ola Are Considering Using India's Creepy National ID Database*, BUZZFEED (Jul. 19, 2017), https://www.buzzfeed.com/amphtml/pranavdixit/airbnb-uber-and-ola-may-start-using-aadhaar-indias.

41. Kessler, *supra* note 39.

42. Social psychology research demonstrates that in conditions of high ambiguity, people are more likely to fall back on stereotypes as heuristics that guide their behavior. *See* Samuel L. Gaertner & John F. Dovidio, *Understanding and Addressing Contemporary Racism: From Aversive Racism to the Common Ingroup Identity Model*, 61 J. SOC. ISS. 615, 621 (2005).

instance, someone with strong negative biases against members of a particular ethnicity may find those stereotypes neutralized by cues about that person's membership in a common group—even if those cues are themselves stereotypic in nature.[43] Behaviors and traits that "attenuate perceptions of threat" from a stereotyped group are sometimes called "disarming mechanisms"[44]; membership in a particular group may suggest the presence of such counter-stereotypical traits that may ultimately mitigate the effects of a primary bias. In addition, if restrictive community composition creates the impression that platform users are members of a cohesive "in-group," such identification might lend users a sense of common identity, overriding biases among group members based on other factors.[45]

At the same time, understanding a platform to be restrictive in some way could have the opposite effect on users by *encouraging* biased judgments, potentially by normalizing the idea that the platform is itself "exclusive" or elite, subduing norms of nondiscrimination in members' interactions. Users may thus feel emboldened to rely even more upon stereotypes in their interactions on a platform.

In practice, the effects of community composition interventions seem likely to depend on users' recognition of these constraints (e.g., are members aware of the barriers to entry into the user base?) and the social associations primed by such exclusions and inclusions (e.g., membership in a shared university community may impart strong positive associations). To the extent that such interventions operate to create a group identity, they may facilitate positive interactions among members of the group.[46]

---

43. *See* David S. Pedulla, *The Positive Consequences of Negative Stereotypes: Race, Sexual Orientation, and the Job Application Process*, 77 SOC. PSYCHOL. Q. 75 (2014) (discussing how counter-stereotypical information can alleviate discrimination by providing a counterweight to stereotypes associated with a particular group). Interestingly, counter-stereotypical cues need not necessarily be positive in nature to alleviate negative stereotypes. Pedulla demonstrates empirically that stereotypes about gay men may negatively impact their perceived employability when the men are assumed to be white—but may actually have *positive* consequences for gay black men's perceived employability. Pedulla posits that the stereotype of gay men as weak counteracts the stereotype of black men as threatening, resulting in a net benefit in perceived employability, rather than a "double disadvantage," for this marginalized group.

44. Robert Livingston & Nicholas Pearce, *The Teddy Bear Effect: Does Babyfaceness Benefit Black CEOs?*, 20 PSYCHOL. SCI. 1229, 1229 (2009).

45. In social psychology, the *common in-group identity model* proposes that the creation of such "superordinate" group identifications can be an effective means of reducing inter-group biases. *See* Samuel L. Gaertner et al., *The Common Ingroup Identity Model: Recategorization and the Reduction of Intergroup Bias*, EUR. REV. SOC. PSYCHOL. 4(1): 1–26 (1993).

46. Gaertner & Dovidio, *supra* note 42, at 629–30.

3. Community policies and messaging

Platforms send a variety of messages to their users about what types of conduct are permissible and use multiple methods to communicate these expectations. These tools range from community guidelines and terms of use (which may be styled as voluntary agreements or mandatory commitments), to required trainings on expected norms of conduct, to other forms of messaging and imagery both on and off the platform. Governance of user behavior through these strategies ranges from explicit rules backed by sanctions to persuasive communication of platform-espoused norms.

Community guidelines and terms of use may explicitly enjoin users from biased interactions on platforms. Some platforms style such policies as "commitments" and incentivize or require users to engage directly with them. For instance, Airbnb's nondiscrimination review requires all users to "affirm and uphold the Airbnb Community Commitment" before using the platform—which commits users "to treat all fellow members of this community, regardless of race, religion, national origin, disability, sex, gender identity, sexual orientation or age, with respect, and without judgment or bias"[47]—as well as to accede to a more detailed nondiscrimination policy, which specifies actions that Airbnb hosts may and may not take.[48] That policy notes that hosts who violate it can be suspended from platform use.[49] Airbnb also provides unconscious bias training for its hosts and asserts it will "work to highlight" hosts who undergo it.[50]

Platforms may also style community guidelines as "pledges," which operate both to cultivate desired norms for interaction *and* to serve a signaling function among the user base. For example, Daddyhunt—a location-based dating app for sexual minority men[51]—encourages its members to "live stigma-free" with respect to dating others regardless of HIV status. A user is not required to pledge to live stigma-free in order to use the platform; however, if he decides to do so, an indicator is attached to his profile (see Figure 1).[52] The founder of Daddyhunt suggests that such a

47. Murphy, *supra* note 18, at 10.

48. For example, hosts may not prohibit the use of a guest's mobility devices but *may* require guests to obey restrictions related to keeping a Kosher kitchen. *Id.* at 27–32.

49. *Id.* at 32.

50. Murphy, *supra* note 18, at 22; *see also supra* Part II.A.1 (critiquing implicit bias training with respect to employees).

51. DADDYHUNT, http://www.daddyhunt.com (last visited July 15, 2017).

52. *See infra* Part II.B.4 (noting the use of profile indicators, like badges, more generally).

feature is designed to "foster a nicer and less judgmental environment for men to meet men."[53]

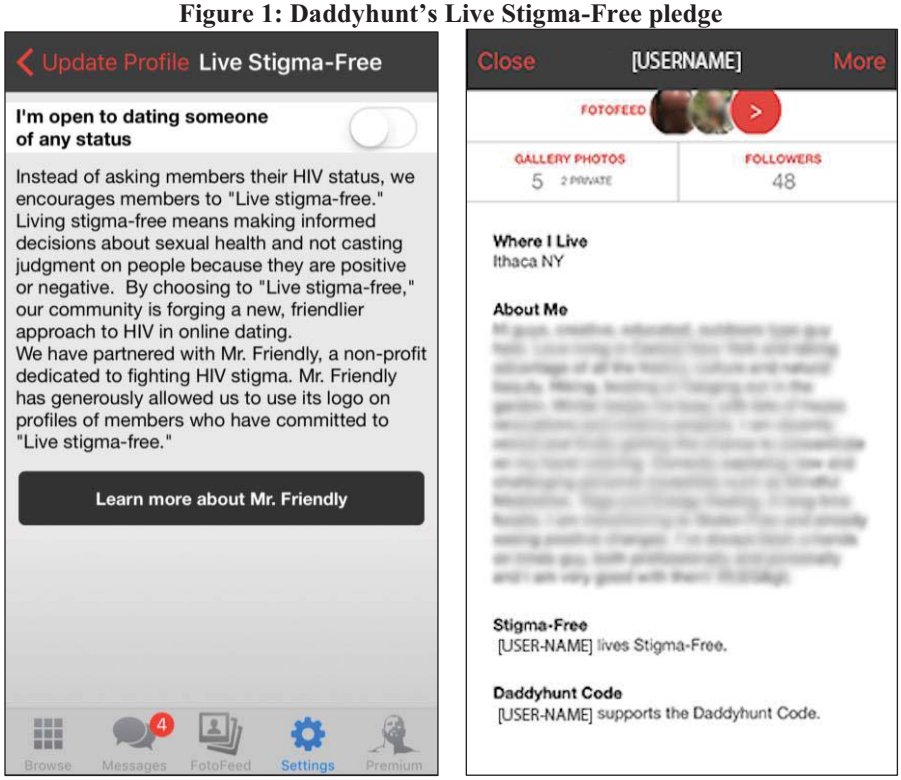
The presence of such a feature ostensibly serves two functions. First, it gives users a tool to learn more about other users' attitudes and behaviors from their profiles, potentially reducing experiences of discrimination and unwelcoming interactions. In addition—even without being required for all users—the presence of the feature serves a broader norm cultivation function by normalizing social interaction with HIV-positive users. Moreover, it represents an interesting alternative means of communicating information about HIV status on Daddyhunt. The platform does not explicitly ask users to disclose HIV status as an element of the user profile,[54] perhaps in light of concerns about increasing stigma by asking such a question directly.[55]

53. Interview with Carl Sandler, CEO of MINSTER, DIGITAL CULTURE & EDUC. (Jul. 17, 2014), http://www.digitalcultureandeducation.com/uncategorized/sandler_html/ (referring to an analogous feature on a related app, MISTER).

54. *See infra* Part II.B.3 on the information revealed in user profiles.

55. In a related vein, the site DUDESNUDE (https://dudesnude.com) opted to create an HIV-friendly community called Poz (short for "positive") rather than asking users about HIV status directly, noting that "not answering the question [about HIV status] may be interpreted as dodging the issue, or putting people in the position where they have to lie." SAN FRANCISCO AIDS FOUNDATION, BUILDING HEALTHY ONLINE COMMUNITIES MEETING REPORT 2 (2014).

Figure 1: Daddyhunt's Live Stigma-Free pledge



Community policies can also be communicated less directly through messaging and imagery, both on and off the platform. For instance, a platform's public statements and advertising can communicate desired norms and evince a desire to attract a user base that shares those norms. Airbnb aired a television advertisement during Super Bowl LI that displayed a diverse range of faces and opined that "[w]e believe no matter who you are, where you're from, who you love or who you worship, we all belong."[56]

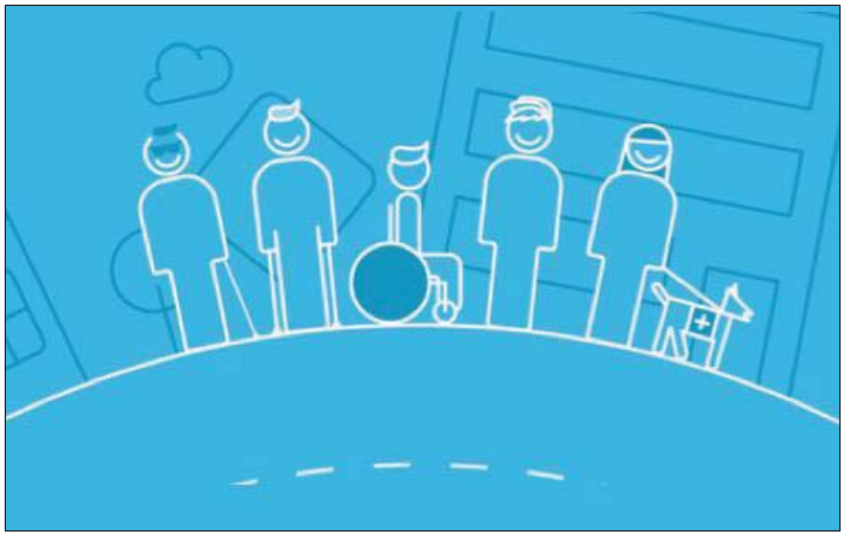
Language and imagery on a site or app may function similarly by affecting how users perceive the norms of transaction. For example, a task site that uses gendered language or images (say, of men assembling furniture) might cue users to view certain categories of people as more appropriate candidates for particular jobs. TaskRabbit, for instance, advertises itself as a tool to "[b]ook a top-rated handyman,"[57] though there

56. Katie Benner, *In Airbnb's Super Bowl Ad, Implied Criticism of Trump's Travel Ban*, N.Y. TIMES (Feb. 6, 2017), at B3.

57. TaskRabbit, http://www.taskrabbit.com (last visited July 15, 2017).

are a number of handywomen working through the platform.[58] Lyft's website features a video on its anti-discrimination policies,[59] which contains imagery of a variety of users with disabilities (including a user in a wheelchair and another with a service dog), providing suggestive visual messaging of the range of users to be welcomed on the platform. The short-term rental site Innclusive[60] describes itself as a "new platform where people of all backgrounds can travel and stay with respect, dignity, and love"[61] and specifically describes the founder's experiences of discrimination on Airbnb as the site's motivation. Even outside of the explicit context of discrimination, visual and textual messaging on a site can cultivate community norms. For instance, Grindr's app includes a "Sexual Health FAQ" that is presented in the context of setting up a user profile. The resources linked to through the FAQ include information on safe sex with HIV-positive partners, potentially reducing such users' stigma on the platform.

Figure 2: Image from Lyft's anti-discrimination policies webpage



58. Elana Lyn Gross, *What It's Like to Be A Female Handywoman on TaskRabbit*, FORBES (Apr. 3, 2017), https://www.forbes.com/sites/elanagross/2017/04/03/what-its-like-to-be-a-female-handywoman-on-taskrabbit/#1828f19115f5.

59. Anti-Discrimination Policies, LYFT, https://help.lyft.com/hc/en-us/articles/214218517-Anti-Discrimination-Policies.

60. INNCLUSIVE, https://www.innclusive.com (last visited July 15, 2017).

61. Our Story, INNCLUSIVE, https://www.innclusive.com/our-story (last visited Mar. 13, 2018).

Community guidelines and messaging can help to address bias in many different ways. Most obviously, published guidelines can offer platforms a consistent basis upon which to assess user behavior and punish those who violate the rules. Should a platform explicitly forbid discriminatory conduct, it could sanction users who engage in such behavior. Efforts to inform users of these guidelines, however, can also deter users from engaging in prohibited behavior in the first place. In such cases, users would consciously self-regulate, abstaining from intentional discrimination for fear of punishment. In contrast, platforms might rely on messaging to change users' underlying beliefs about inclusion, diversity, and non-discrimination. In publicly committing the community to such values, platforms aim to foster such commitments among individual users, encouraging users to shed their prejudicial or biased beliefs. At the same time, messaging of this sort can also invite potential users who hold these beliefs to join the community, thereby changing the composition of the community to include more users consciously committed to keeping their prejudices and biases at bay. Platforms might be more circuitous, however, engendering greater comfort among diverse users by simply exposing users to images and messaging that undermine stereotypes and stigmas. Rather than targeting consciously held beliefs, these interventions address implicit associations, prompting changes in attitudes about which users may remain largely unaware.

B. STRUCTURING INTERACTIONS

Platforms have immense power to scaffold users' encounters with one another. They can offer cues to users about conduct norms in the moment of exchange, just as biases are likely to surface. They can structure markets to determine the degree of choice and discretion users have about their exchange partners, and control what users learn about each other's characteristics throughout an encounter—potentially restricting a user's propensity or ability to discriminate. They can also offer users opportunities to evaluate each other's performance (though these evaluations may themselves be marked by bias) and can make indicia of reputation visible to other potential exchange partners.

1. Prompting and priming

Platforms may prompt users to reflect on their behavior with the intent to minimize bias, often by providing users with some information or pop-up dialog (known in web design as an *interstitial*) that must be acceded to before proceeding with a particular communication or transaction. These measures can take several forms and may be more or less explicit about the reason for the intervention. They may remind users to abide by community

guidelines or a code of conduct[62] to which they have previously agreed, hence priming users to refrain from exhibiting bias in the present transaction by making anti-bias commitments more top-of-mind.[63] Such prompts may be triggered to appear only when likely biased behavior is detected, by default for all interactions, or when some other conditions are met.

For example, the neighborhood-based social networking site Nextdoor developed numerous design strategies to alleviate racial profiling by users reporting suspicious activity in their neighborhoods.[64] Among these was the use of an interstitial prompt (see Figure 3, below) that gives users a variety of tips intended to minimize the role of bias in the report (e.g., "Give a full description, including clothing, to distinguish between similar people. Consider unintended consequences if the description is so vague that an innocent person could be targeted.").[65] Similar approaches have been used in addressing online harassment and incivility. The discussion platform Discourse prompts new users with reminders of community civility guidelines just as they begin to post content to the site.[66] Yik Yak, a social media app in which users post anonymous "Yaks"—short messages visible to others in their local area, often college campuses—prompts users to "pump the brakes" via an interstitial message if the Yak in question seems to contain threatening or offensive language.[67]

Evidence from academic studies lends credence to these types of interventions. Mazar et al. show that people's propensity to lie is affected not by whether they know or believe that dishonest behavior is morally wrong, but "whether they think of these [moral] standards and compare their behavior with them *in the moment of temptation*."[68] In their study, priming research participants with reminders of honor codes and religious edicts just before completing a task deterred cheating behavior. More recent work has shown that immediately censuring people for violations of some norm can also reduce the incidence of such behavior. An experiment on Twitter deployed bots to respond to the use of racial slurs by socially sanctioning

62. *See* Part II.A.3, *supra*.

63. Fisman & Luca, *supra* note 1.

64. *See* Hempel, *supra* note 24. Nextdoor's interventions are discussed in more detail in Part II.C.2, *infra*.

65. Hempel, *supra* note 24.

66. *See* Jeff Atwood, *The "Just in Time" Theory of User Behavior*, CODING HORROR (Jul. 17, 2014), https://blog.codinghorror.com/the-just-in-time-theory/.

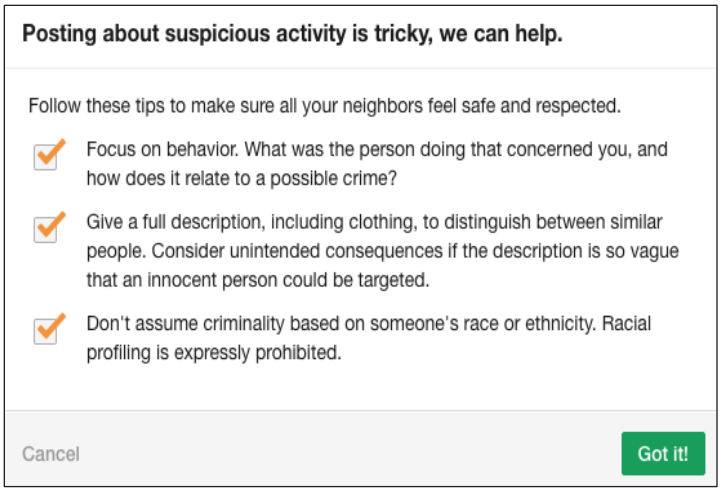
67. Jonathan Mahler, *Who Spewed That Abuse? Anonymous Yik Yak App Isn't Telling*, N.Y. TIMES (Mar. 8, 2015), https://www.nytimes.com/2015/03/09/technology/popular-yik-yak-app-confers-anonymity-and-delivers-abuse.html.

68. Nina Mazar et al., *The Dishonesty of Honest People: A Theory of Self-Concept Maintenance*, 45 J. MKTG. RES. 633, 635 (emphasis added).

users in an @-reply to the offensive message (e.g. "Hey man, just remember that there are real people who are hurt when you harass them with that kind of language."). The experiment found that such sanctions could reduce future propensity to harass, particularly when the bots were perceived to be white males with a large number of Twitter followers.[69]

There remains, however, ongoing debate in social psychology regarding the degree to which interventions aimed at making decisions more deliberative can counter biased judgment.[70] So far, evidence is mixed about the effectiveness of "getting people to think more about, or to attend more closely to, their objectives in an inter-racial interaction" as a means of mitigating the influence of *implicit* bias.[71]

Figure 3: Nextdoor's interstitial prompt, intended to minimize bias



69. *See* Kevin Munger, *Tweetment Effects on the Tweeted: Experimentally Reducing Racist Harassment*, POL. BEHAV., (Nov. 11, 2016), https://doi.org/10.1007/S11109-16-9373-5.

70. *See* Jennifer L. Eberhardt, *Imaging Race*, 60 AM. PSYCHOL. 181, 181–2 (2005) ("Determining the extent to which racial bias can be automatically triggered versus deliberately controlled is a fundamental issue in social psychology. Better understanding this tension may improve not only theories of social cognition but also interventions designed to reduce bias and minimize racial inequities").

71. Anthony G. Greenwald & Linda Hamilton Krieger, *Implicit Bias: Scientific Foundations*, 94 CAL. L. REV. 945, 962 (2006) (reviewing studies).

2. How users learn about one another

By necessity, platforms scaffold the process by which users find one another, and different design choices can leave more or less leeway for users to exercise biased preferences. Platforms often function like markets, helping supply find demand (and vice versa). Platforms employ a wide range of techniques to facilitate this process. Some assume a relatively passive role in matching supply and demand (leaving a good deal of the process of finding an appropriate partner to the transacting parties themselves), while others take a more active role (automating much of the process of pairing riders and drivers, for example). Some provide users with tools to search and sort; others provide users with recommendations. In many cases, the marketplace that users confront on these platforms is a rank-ordered list; platforms cannot help but play a crucial part in determining what potential exchange partners are listed, and in what order.[72] Broadly speaking, then, platforms structure how users find one another by determining who is in a position to search for exchange partners, how much discretion users have in determining with whom to transact, and what tools are provided to users to facilitate the search process.

When deciding whether to put specific users in the privileged position of choosing with whom to interact, platforms create very different opportunities for discrimination to occur between users. Structurally, platforms can allow buyers to choose among sellers, allow sellers to choose among buyers, or allow both sellers and buyers to choose among themselves. A platform that gives job-seekers the opportunity to find and contact potential employers necessarily ensures that employers cannot limit their search to male candidates *ex ante* (despite the fact that employers may subsequently reject all female applicants) because employers are not the parties doing the searching. In contrast, when employers can search for candidates, they might only consider and contact male candidates, denying female candidates an opportunity to even learn about the job. A requirement to accept all comers in this case could mitigate against the possibility that candidates might reject offers for prejudicial reasons of their own, but such a requirement would also be unworkable in many cases (e.g., compelled work among freelancers).

Platforms can also be designed to provide sellers or buyers with a right of refusal when approached by the other—or deny any such discretion.

72. *See* James H. Moor, *What is Computer Ethics?*, 16 METAPHILOSOPHY 266, 274 (1985) (noting that designers of a search engine cannot avoid making choices about how results are ordered and displayed).

eBay, for example, allows buyers to choose among any sellers of the same or similar item, while sellers must accept all comers.[73] Fiverr, a platform for freelancers, has job-seekers (sellers) list their skills so that employers (buyers) can approach them, though job-seekers retain the right to refuse any particular offer. In contrast, Upwork, another platform for freelancers, features job listings where job-seekers (sellers) choose among job-listers (buyers), where the ultimate hiring decision still rests with the job-lister. Airbnb generally follows this format as well (giving hosts the right to refuse guests' housing requests), though the platform also provides an "Instant Book" feature that allows travelers to book a stay at someone's home without the host having a chance to review the request. The company has recognized that forcing buyers to accept all comers can mitigate against the possibility of bias in assessing users who make contact.[74] In other contexts, both transacting parties have the power to refuse offers as they please. On online dating platforms like OKCupid, the distinction between buyers and sellers breaks down and all users are in a position to find, approach, and accept or reject one another. In these cases, the decisions made by either party—either in who to contact or who to accept—could be biased.

At the same time, platforms frequently attempt to relieve buyers and sellers of much of the burden of finding an appropriate counterparty. At the extreme, some platforms automate the process of matching supply and demand, often using algorithms that pair people according to fixed criteria or patterns learned from historical data. Uber, for instance, does not present riders with a list of nearby drivers from whom riders may choose. Instead, Uber shields from view the process by which the company secures a driver for the specific rider and simply delivers a car to the passenger.[75] Uber does,

73. eBay sellers can, however, cancel bids from or sales to specific buyers, once they have learned about buyers. While the platform lists a small number of reasons for why sellers might want to do this (e.g., "A bidder contacts you to back out of the bid; You cannot verify the identity of the bidder after trying all reasonable means of contact; You end your listing early."), sellers seem to be at liberty to do this whenever they like. Sellers can also block specific buyers from even bidding on items, but sellers need to add specific usernames to a blacklist one-by-one. Managing Bidders and Buyers, eBay Help, http://pages.ebay.com/help/sell/manage_bidders_ov.html#block (last visited September 6, 2017).

74. *See* Murphy, *supra* note 18, at 22 ("Instant Book makes it easier for guests to be accepted by hosts on the platform if they meet some basic qualifications, and hosts can set preferences that serve the purpose of automatically filtering guests, including whether the listing is pet-friendly, suitable for events, or features particular amenities. More importantly, Instant Book reduces the potential for bias because hosts automatically accept guests who meet these objective custom settings they have put in place").

75. While Uber presents users requesting a ride with a map depicting cars in the area, such maps may not represent actual drivers available for pickups. Further, users have no

however, send notifications to nearby drivers who have the option to accept or reject the request. At no time do drivers see *all* requests in the area; Uber instead doles out requests one by one. From the perspective of riders, Uber fully automates the matching of supply and demand; from the perspective of drivers, Uber severely constrains information about nearby demand (to one request at a time), likely to pressure drivers to accept *any* request, given uncertainty about future requests. Notably, the company also withholds information about the intended destination of the passenger requesting a ride, also to limit the flow of information that might dissuade a driver from accepting the request.[76] And to top it off, Uber will penalize drivers who reject too many requests.[77]

Where this strategy is successful, Uber can come close to pairing riders and drivers in an almost fully automated manner. And doing so has been perceived as helping to mitigate bias.[78] Riders and drivers will have little opportunity to make biased assessments of each other because they never engage in any kind of negotiation or interaction; they are simply paired with one another based on some—ideally—rational criteria set by the platform. At the same time, such behavior betrays the belief that platforms operate as free and open markets.[79]

Fully automated matching will not work for all types of platforms. Users may not know exactly what they want in a counterparty or cannot express all their preferences and requirements explicitly or in advance. The process of exploring what is available on a platform may be the process by which users figure out what they want. Platforms facilitate this process by providing recommendations, rank ordering options, offering search functionality, and furnishing users with granular controls to sort and filter results in any number of ways. How platforms present users to each other can dramatically affect whether patterns of interaction exhibit bias. To

---

way of choosing among the cars depicted on the map. Alex Rosenblat, *Uber's Phantom Cabs*, MOTHERBOARD (Jul. 27, 2015), https://motherboard.vice.com/en_us/article/ubers-phantom-cabs.

76. Drivers and riders might get around this by cancelling on one another after learning about their assigned rider or driver. *See infra* note 158.

77. *See* Alex Rosenblat & Luke Stark, *Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers*, 10 INT'L J. COMM. 3758, 3762 (2016).

78. *See* Ruth Igielnik & Monica Anderson, *Ride-Hailing Services are Seen as a Benefit to Areas Underserved by Taxis*, PEW RES. CTR. (Jul. 25, 2016), http://www.pewresearch.org/fact-tank/2016/07/25/ride-hailing-services-are-seen-by-minorities-as-a-benefit-to-areas-underserved-by-taxis/.

79. *See* Tim Hwang & Madeleine Clare Elish, *The Mirage of the Marketplace*, SLATE (Jul. 27, 2015), http://www.slate.com/articles/technology/future_tense/2015/07/uber_s_algorithm_and_the_mirage_of_the_marketplace.html.

begin, if the platform relies on historical patterns of successful user interaction to guide its future recommendations, these suggestions might reproduce or even exacerbate the prejudices and biases that influenced previous users' decisions to interact with others—and their assessments of those people.[80] That said, recommendations can also direct users to focus on others who are more appropriate counterparties than users' biased heuristics might lead them to believe, or than traditional searching methods might uncover. Indeed, such recommendations might even incorporate diversity metrics,[81] which would aim to ensure that recommendations span a range of appropriate users across numerous identified groups. Platforms that aim to generate rank ordered lists that feature descending "best matches" might serve a similar function if the platform computes the rank by looking at demonstrably relevant factors as well as diversity metrics.[82]

Users might also have the ability to perform different types of searches, seeking out a counterparty with specific and discrete qualities (selected using dropdown menus or radio buttons, for example) or by entering freeform text into a dialogue box. Platforms might provide further control to users in the form of sorting mechanisms or filters, allowing users to change the rank order of people in the search results according to certain criteria or remove certain people completely. As a condition of providing these kinds of granular controls, platforms must determine the discrete criteria upon which they will allow users to sort and filter. Tools that grant users greater control over the set of people they will see when searching for a counterparty can both empower and embolden users to discriminate (and may expose platforms to liability for violation of underlying civil rights laws). While online dating platforms are not subject to any such laws, they vary dramatically in whether they allow users to search, sort, or filter by race, ethnicity, or religion, for example.[83] On Match.com, one of the first

80. *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 681–84 (2016). *See also* Aniko Hannak et al., *Bias in Online Freelance Marketplaces: Evidence from TaskRabbit and Fiverr*, Proc. Conf. on Computer-Supported Cooperative Work and Social Computing (2017).

81. *See, e.g.,* Saúl Vargas & Pablo Castells, *Rank and Relevance in Novelty and Diversity Metrics for Recommender Systems*, PROC. FIFTH ACM CONF. RECOMMENDER SYS. 109 (2011).

82. In most cases, platforms that present a range of options to users cannot avoid presenting a list ordered in some particular way. *See* James H. Moor, *What is Computer Ethics?*, 16 METAPHILOSOPHY 266, 274 (1985).

83. *See, e.g.,* Carrie Weisman, *The Casual Racism of our Most Popular Dating Apps*, SALON (Sep. 28, 2015), https://www.salon.com/2015/09/28/sexual_racism_why_people_say_racist_things_on_dating_apps_partner; Patrick Strudwick, *The Founders of This Gay Dating App Won't Stop You Searching By Race*, BUZZFEED (Feb. 9, 2016),

questions posed to new users concerns their ethnic preferences in a partner; later on, users can filter search results on the basis of ethnicity. Yet other sites do not solicit these preferences or allow users to filter accordingly, despite the fact that users' preferences might still guide their ultimate dating choices.[84] And while platforms might not want to limit users' freedom of choice when it comes to romantic and sexual decisions, they may nevertheless refrain from collecting information and providing tools that allow users to effectively remove members of entire racial or ethnic groups from the apparent marketplace of potential partners.

3. What users learn about one another

In designing the interfaces through which users interact, platforms exercise enormous control over the type of information made available to transacting parties. What users see when hiring a worker to complete a task, getting in touch with the owner of a rental property, or contacting a prospective date, for example, can significantly affect how users judge these counterparties. In offline interactions, people cannot help but draw all sorts of inferences about others from readily available indicators. For example, a job applicant may (perhaps unwittingly) signal his personality through the clothing he wears or the way he carries himself. In the mediated interactions facilitated by platforms, such details might not be communicated to users at all—or supplemented by others. Indeed, platforms can make all sorts of choices about what information is disclosed, what is withheld, and how trustworthy that information is deemed to be.[85] For the purposes of online interactions, users are the sum total of the signals that platforms transmit between parties. Platforms, therefore, have powerful capacities to determine what their users learn about one another. This section details four ways in which they do so: by encouraging or requiring the disclosure of user information; by withholding user information; by structuring the input of

https://www.buzzfeed.com/patrickstrudwick/this-is-how-gay-dating-app-bosses-defend-racial-filtering. *See also* Elizabeth F. Emens, *Intimate Discrimination: The State's Role in the Accidents of Sex and Love*, 122 HARV. L. REV. 1307, 1322–23 (2009) (describing a range of dating websites' practices allowing, or requiring, indication of a user's own race and capacity to search for potential partners by race).

84. *See* Russell K. Robinson, *Structural Dimensions of Romantic Preferences*, 76 FORDHAM L. REV. 2787, 2792 (2007).

85. *See* Nicole B. Ellison et al., *Profile as Promise: A Framework for Conceptualizing Veracity in Online Dating Self-Presentations*, 14 NEW MEDIA & SOC. 45, 54 (2011) (describing online platforms as "reduced-cue environments" in which "online daters cannot 'show' characteristics such as age, gender, or location, [and so] are forced to 'tell' them through text-based communication").

user information; and by linking user information to external sources for authentication.

First, some platforms encourage or require[86] users to disclose personal information about themselves that fills them out as people, even if such information is not directly germane to the substance of the transaction. For instance, Airbnb allows users to submit 30-second profile videos and suggests that they include "a fun fact about yourself or why you love Airbnb"; eBay implores users to share "what you're passionate about."[87] TaskRabbit's "about me" section encourages taskers to enter information about hobbies and interests, in response to prompts like "When I'm *not* tasking . . . ."[88] In addition to personal profiles, many platforms encourage or require users to include profile photos or videos of themselves. Airbnb tells users that "[c]lear frontal face photos are an important way for hosts and guests to learn about each other. It's not much fun to host a landscape! Please upload a photo that clearly shows your face."[89]

The disclosure of additional information about a user may serve to mitigate bias. Information that leads others to see a user as a "whole person" might lead them to rely less on discrete signals (gender, ethnicity, etc.) in choosing partners with whom to transact. A recent study of Airbnb host profiles found that the majority of hosts disclose information about their career or education (e.g., the host's current job and where she went to school) and their interests and tastes (e.g., favorite books, music, and hobbies).[90] Moreover, the study found that hosts with longer profiles and who discuss more topics in their profiles are perceived as more trustworthy, and that such perceived trustworthiness can influence guests' choices in deciding with whom to stay.[91] Profiles may provide opportunities to signal

86. Even if platforms do not require users to disclose particular types of information, users who decline to include such information may be subject to adverse inference. *See* Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U.L. REV. 1153, 1176–77 (explaining that users who refrain from disclosing information will be assumed to possess undesirable qualities) (2011).

87. *How Do I Make a Profile Video?*, AIRBNB, https://www.airbnb.com/help/article/213/how-do-i-make-a-profile-video (last visited Mar. 18, 2018).

88. Screenshots on file with authors.

89. Airbnb signup process [screenshot on file with authors].

90. Xiao Ma et al., *Self-Disclosure and Perceived Trustworthiness of Airbnb Host Profiles*, PROC. OF THE CONFERENCE ON COMPUTER-SUPPORTED COOPERATIVE WORK & SOC. COMPUTING, March 2017, at 2400–01.

91. *Id.* at 2407.

counter-stereotypical information that may mitigate biases based on protected characteristics.[92]

However, the provision of personal information can also exacerbate bias on platforms, if people rely on such information to render biased decisions. Photos, of course, communicate a great deal of information, and lend themselves to inferences about gender, race, age, and other protected class characteristics. Even information about hobbies, interests, geographic location, or other features may function as proxies for such characteristics, even when they are not explicitly revealed.

Therefore, a second emerging strategy for combating bias is to purposefully *withhold* certain types of user information from other users, at least until a transaction is completed. This strategy is particularly salient for user photos and names, which can strongly indicate race and gender without providing much additional information relevant for choosing an exchange partner, to the great detriment of marginalized groups.[93] An experimental study of racial bias on Airbnb found that prospective guests with distinctively black names were 16% less likely to have their rental requests accepted than equivalent guests with white names,[94] precipitating the recommendation that Airbnb eliminate photos and substitute pseudonyms (such as "Airbnb Host" and "Airbnb Guest") for users' real names.[95] (After

92. Writer Brent Staples writes of walking down the street at night in Chicago as a young black man and "whistl[ing] popular tunes from the Beatles and Vivaldi's *Four Seasons*" to counter the negative stereotypes white pedestrians had about him as a threatening figure. CLAUDE M. STEELE, WHISTLING VIVALDI: HOW STEREOTYPES AFFECT US AND WHAT WE CAN DO 6 (2010). Similarly, the presentation of counter-stereotypical indicators in a profile may be a strategy to alleviate negative treatment in online spaces. Of course, Staples's perceived need to counteract others' stereotypes in order to exist in public space represents an enormous and unfair burden wrought by discrimination, and it must be acknowledged that the judgments rendered on the basis of counter-stereotypical information are likely themselves inflected by bias, as well. *See supra* Part II.A.2.

93. *See* Jennifer L. Doleac & Luke C.D. Stein, *The Visible Hand: Race and Online Market Outcomes*, 123 ECON. J. F469 (2013) (finding experimental evidence on an online classified marketplace that black sellers had worse market outcomes, based on photographs that included a dark-skinned or a light-skinned hand holding an identical product); Ian Ayres et al., *Race Effects on eBay*, 46 RAND J. OF ECON. 891, 910 (2015) (finding, similarly, that baseball cards held by dark-skinned hands generated lower auction prices on eBay than comparable cards held by light-skinned hands).

94. Benjamin Edelman et al., *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, 9 AM. ECON. J.: APPLIED ECON. 1 (2017).

95. Benjamin Edelman, *Preventing Discrimination at Airbnb* (Jun. 23, 2016), http://www.benedelman.org/news/062316-1.html. *See also* Sarah K. Harkness, *Discrimination in Lending Markets: Status and the Intersections of Gender and Race*, 79 SOC. PSYCH. Q. 81 (2016) (finding that "gender and race significantly affect lenders'

an exchange is finalized, it may be more useful to reveal photos and names—for instance, to help transaction partners find and identify one another offline.[96])

In response to this study, Airbnb agreed to "experiment with reducing the prominence" of user photos on its platform—though it stopped short of concealing them entirely, based on the notion that "Airbnb guests should not be asked or required to hide behind curtains of anonymity when trying to find a place to stay. . . . [T]echnology shouldn't ask us to hide who we are."[97] (The authors of the Airbnb experimental study subsequently released a browser plugin, Debias Yourself, which obscures users' faces and names during Airbnb transactions; the plugin's creators encourage Airbnb hosts and guests to indicate their use of the plugin in their user profiles and photos, and the authors provide sample text to this effect, as well as a badge indicating such use to be included on profile photos.[98])

The practice of withholding certain information from a decision-maker in order to diminish the potential for bias to enter into her decisions has longstanding analogues in offline employment contexts. In one well-known study, symphony orchestras that obscured auditioning musicians behind a screen saw a marked increase in the number of women hired for positions—because decision-makers' evaluations were, presumably, less inflected by bias about the inferiority of women musicians[99]—and a number of sites and apps have imported this idea to other contexts of employment-related decision-making, by concealing certain candidate characteristics or otherwise restructuring the candidate assessment process.[100] A number of legal rules, as well as social norms, militate against requesting (or, in some cases, revealing) various types of information, in the interest of avoiding any possibility of making decisions based on contextually improper (or illegal) considerations: for instance, employers may not inquire as to a

---

funding decisions" on a peer-to-peer lending site "because they alter lenders' status beliefs about" applicants).

96. Some platforms reveal photographs of users only once a user is far into a transaction (or has completed it). The vacation rental site HomeAway withholds profile photos of hosts on search results pages, unlike Airbnb. Ray Fisman & Michael Luca, *Fixing Discrimination in Online Marketplaces*, HARV. BUS. REV. (Dec. 2016), https://hbr.org/2016/12/fixing-discrimination-in-online-marketplaces.

97. Murphy, *supra* note 18, at 23.

98. DeBias Yourself, http://debiasyourself.org/get.html. *See also infra* Part II.B.4 on badges/profile credentials.

99. *See generally* Claudia Goldin & Cecelia Rouse, *Orchestrating Impartiality: The Impact of "Blind" Auditions on Female Musicians*, 90 AM. ECON. REV. 715 (2000).

100. *See* Mundy, *supra* note 26 (describing a range of "anti-bias apps" in hiring).

prospective employee's disability, and colleges can lose federal funds if they request information about an applicant's marital status.[101]

However, even well-intentioned limitations on information collection can have unanticipated detrimental consequences. Over the past few years, the federal government, along with a number of cities, states, and private employers, has promulgated "ban the box" policies that prohibit asking on job applications whether prospective hires have criminal offense records. The intuition behind such policies is that employers are likely to be highly biased against former offenders, and that job seekers who answer such a question honestly are likely to be dismissed out-of-hand, making it nearly impossible for ex-offenders to find employment; therefore, these rules are intended to "level the playing field" between those with and without criminal records in the hiring process.[102] However, such measures have had a perverse consequence. Rather than refraining from consideration of offense records in their absence, employers are more likely to fall back on information that is *correlated* with offense records—namely, information about a candidate's race. Hence, ban-the-box measures can lead to statistically *worse* outcomes for black and Hispanic job candidates.[103] Thus, in place of withholding criminal history information, some economists recommend providing affirmative indicia of reliability, such as "employability certificates" that "signal an individual's work-readiness."[104]

---

101. *See* Adam M. Samaha & Lior Jacob Strahilevitz, *Don't Ask, Must Tell—And Other Combinations*, 103 CAL. L. REV. 919, 946 (2015). *See also* Lior Jacob Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. L. REV. 1667, 1711–12 (2008) (discussing law's use of "curtains" and "search lights" to, respectively, reduce the observability of certain types of information, or draw attention thereto, for policy purposes).

102. Jennifer L. Doleac, *"Ban the Box" Does More Harm than Good*, BROOKINGS INSTITUTION (May 31, 2016), https://www.brookings.edu/opinions/ban-the-box-does-more-harm-than-good/; Note that employers following ban-the-box policies typically *may* ask prospective hires about their pasts at the interview stage; at that point, it is assumed that candidates will have more opportunity to explain their situations, and employers will have a "fuller picture" of who the candidate is.

103. *See id. See also* Jennifer L. Doleac & Benjamin Hansen, *Does "Ban the Box" Help or Hurt Low-Skilled Workers? Statistical Discrimination and Employment Outcomes When Criminal Histories are Hidden*, NAT. BUR. OF ECON. RES. WORKING PAPER NO. 22469 (Jul. 2016), http://www.nber.org/papers/w22469; Amanda Agan & Sonja Starr, *Ban the Box, Criminal Records, and Statistical Discrimination: A Field Experiment*, BECKER FRIEDMAN INST. FOR RES. IN ECON. WORKING PAPER NO. 2016–17 (Jul. 2016), http://bfi.uchicago.edu/sites/default/files/research/2016-17.pdf.

104. Jennifer Doleac, *More Job Opportunities, Less Recidivism*, REALCLEARPOLICY (Dec. 15, 2016), http://www.realclearpolicy.com/articles/2016/12/15/more_job_opportunities_less_recidivism.html; Peter Leasure & Tia Stevens Andersen, *The Effectiveness of Certificates of Relief as Collateral Consequence Relief Mechanisms: An*

Furthermore, even when online environments intentionally offer few explicit cues of a user's characteristics, users may nevertheless be able to readily infer (and behave differently based on) those characteristics. For example, an experimental study of users on eBay found that users were able to accurately identify the gender of an eBay seller the majority of the time, even in the absence of user photos, real names, or an explicit profile indicator of gender.[105] The study's authors also found that women sellers on eBay suffered significant penalties for their gender, earning about 80 cents on the dollar earned by male sellers for identical new products.[106]

The eBay study and the ban-the-box case suggest that strategies premised on suppressing information about users, while holding promise for reducing the potential for bias, must be carefully considered in the broader context of what information *is* visible on the platform. Users may readily default to what information is available about a counterparty, resulting in less effective (or potentially even detrimental) interventions.

Third, in addition to the amount of personal disclosure permitted (or required or disallowed), the forms that such presentation is permitted to take may influence its role in supporting users' biases. For instance, structuring information via predefined fields—as opposed, say, to free text—allows platforms to define input categories in advance as well as acceptable inputs for each category. In so doing, platforms may attempt to delimit what information they want to permit users to draw from in making decisions:[107] for instance, by excluding the capability to list one's religion, platforms may attempt to insulate user activity from consideration thereof.[108] However, decisions about how information is structured can also introduce other forms of bias: consider, for instance, asking for a user's gender as a binary

Experimental Study, YALE L. & POL'Y REV. INTER ALIA (Nov. 7, 2016), http://ylpr.yale.edu/inter_alia/effectiveness-certificates-relief-collateral-consequence-relief-mechanisms-experimental; Peter Leasure & Tara Martin, *Criminal Records and Housing: An Experimental Study*, J. EXP. CRIMINOL. (2017); *see also infra* Part II.B.4 on profile badges and credentials.

105. Tamar Kricheli-Katz & Tali Regev, *How Many Cents on the Dollar? Women and Men in Product Markets*, 2 SCI. ADVANCES 1 (2016). The array of goods the seller had for sale seemed to be a reliable proxy for gender, as "the probability of correctly identifying the gender of the seller increased by 5% with every additional item for sale on display on the seller's profile." *Id.* at 6.

106. *Id.* at 1.

107. This is tempered, however, by the aforementioned "ban-the-box" effects, in which users glean signals from correlated variables.

108. However, structuring inputs in this manner may place a platform at a greater risk for liability based on its users' behavior; *see supra* discussion of *Roommates.com*, notes 10–14.

variable, and how such structuring can operate as a vehicle for exclusion of users with other gender identities.[109]

Platforms may also discretize how information is displayed to users at various points in decision processes (i.e., on separate pages of a user interface). "Chunking" involves pulling out specific attributes individually and asking decision-makers to compare across them. In the employment context, the hiring software beApplied "reorders applications horizontally so that reviewers just focus on comparing responses to individual questions. Since applications are also blind, you know you're assessing the quality of each response fairly."[110] The goal of doing so is to minimize "halo effects" from previous knowledge about a candidate (i.e., letting one's judgment be colored by knowledge about a person's gender, age, etc.); in a sense, such discretization is the logical opposite of platforms' "whole person" design strategies described above.

Finally, platforms may authenticate users' identities by linking them to external profiles or by requiring users to use their real names on the platform. Many platforms allow, or require, users to link accounts to a Facebook, LinkedIn, or other social media profile (see Figure 4 below), often in the interest of preventing scams.[111] Others—most notably, Facebook—require that users' profiles use their "real names," as opposed to a pseudonymous handle.[112]

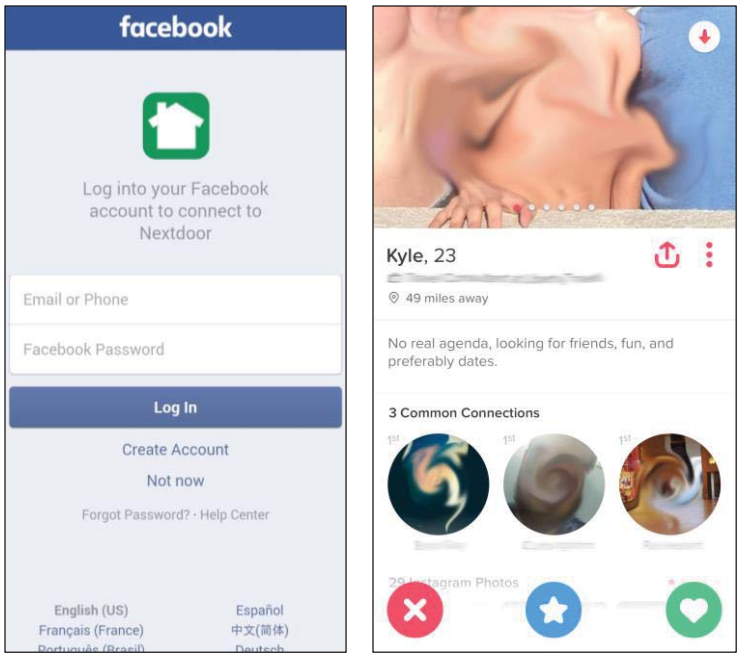
109. Sabrina Fonseca, *Designing Forms for Gender Diversity and Inclusion*, UXDESIGN.CC (Apr. 24, 2017), https://uxdesign.cc/designing-forms-for-gender-diversity-and-inclusion-d8194cf1f51; *see also* discussion of Tinder's gender categories *infra* notes 170–183.

110. BEAPPLIED, https://www.beapplied.com/features (last visited September 6, 2017).

111. For instance, the localized goods exchange app 5miles requires two forms of external identification (phone number, email address, or Facebook profile) to be linked to a user; the related app OfferUp requires Facebook access and a photograph of the user's driver's license. Roy Furchgott, *Decluttering? Yes, There's an App*, N.Y. TIMES (Apr. 7, 2017), https://www.nytimes.com/2017/04/07/realestate/spring-cleaning-and-decluttering-help-apps.html.

112. Facebook's real name policy states that "Facebook is a community where everyone uses the name they go by in everyday life. This makes it so that you always know who you're connecting with and helps keep our community safe." *What names are allowed on Facebook?*, FACEBOOK HELP CENTER, https://www.facebook.com/help/112146705538576 (last visited September 6, 2017).

Figure 4: Nextdoor allows users to authenticate themselves using their Facebook login credentials; Tinder allows users to link their accounts to their Facebook accounts, highlighting if users share friends in common.



Authentication mechanisms might mitigate bias in at least three ways. Linkage with activity on other platforms or with offline identities could coax users into self-modulating their conduct in socially desirable ways, out of a sense of greater accountability for their actions—though whether such accountability would extend to implicit biases is an open question. Second, seeing *other* users' linkages to other arenas might operate as a humanizing signal of their identity as a "whole person" that might mitigate reliance on stereotypes (much like user profile information, discussed *supra*) and increase trust. Finally, certain platforms attempt to cultivate even greater confidence among users by showcasing when they share friends in common on the outside platform through which they have authenticated their identities. For example, Tinder notes the number of Facebook friends that a user shares with the person whose profile the user is viewing. Making such connections explicit might encourage users to consider potential matches that they would have been dismissed instinctively otherwise, potentially on prejudicial or biased grounds. At the same time, identification mechanisms could provide additional fodder on which to base biased decisions. For instance, real name policies might prove detrimental to platform users whose names are strongly associated with particular races or ethnicities, and users may be limited from adopting indicators of identity that make them

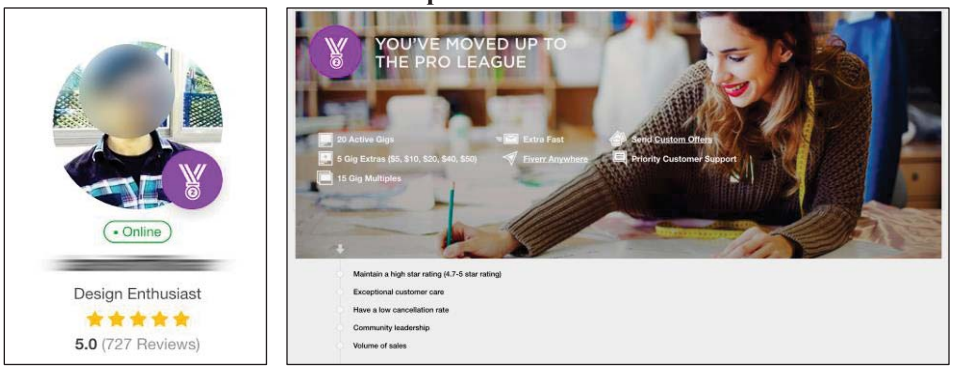
appear less "marked." Identifying common connections can also have the effect of encouraging users to interact with people already in their social network, thereby reproducing disparities in social capital along the lines of race and other protected characteristics.

4. Reputation, reliability, ratings

The strategies described in the previous section help users learn about each other's identities, to decide whether and how to interact with one another. A related set of platform strategies aims to equip users with indicators about what to expect from a transacting partner on the site based on *past behavior*. These indicators can confer a sense of expertise, reputation, or trustworthiness that may increase counterparties' trust in the exchange,[113] and may provide countervailing signals that can mitigate users' implicit biases.

Some indicia of reliability take the form of badges or other graphic elements on users' profiles. Badges may indicate a certain amount of engagement or longevity with a platform (e.g., a certain number of tasks completed), or a certain degree of quality, perhaps operationalized as a high composite rating. The labor marketplace Fiverr, for instance, allows sellers to "level up" based on experience and ratings; when a new level is achieved, a badge is displayed prominently on the user's profile (see Figure 5).[114]

Figure 5: Fiverr displays badges on a user's profile based on experience on the platform



113. Audun Jøsang et al., *A Survey of Trust and Reputation Systems for Online Service Provision*, 43 DECISION SUPPORT SYS. 618, 621–22 (2007); *see also* Part II.A.2 *supra*.

114. FIVERR'S LEVELS, https://www.fiverr.com/levels (last visited September 6, 2017).

Testimonials, references, and reviews may also serve as signals of reliability because they may pertain to a user's general character and reputation. For instance, Airbnb permits users to post "references from your personal network . . . from people who know you well" which "will help other members get to know you"[115], and LinkedIn permits users to offer recommendations[116] and endorsements about another user's skills.[117] Alternatively, these indicators may be based on particular past interactions on the platform; eBay, Airbnb, Etsy, and many other platforms allow users to write reviews of past interactions, and make these reviews visible to the broader user base as a means of broadcasting reputation. A recent field experiment on Airbnb found that booking requests from black guests (as indicated by distinctively African-American names) had a lower acceptance rate than those from white guests; however, when each guest's profile had one positive review, the acceptance rate was almost identical, suggesting that the presence of a review acted as a counter-stereotypical signal that alleviated bias.[118] Matched negative reviews had the same effect at removing disparities in acceptance rates between black and white guests.[119]

One of the most ubiquitous forms of user evaluation involves rating a counterparty on the quality of an exchange, most commonly by assigning them a number of stars. Uber, Lyft, eBay, Instacart, Postmates, and myriad other platforms have ratings systems for evaluation of tasks; individual ratings contribute to a composite rating that is typically displayed on the user's profile, operating as an indicator of reliability and satisfaction.[120] Ratings are typically platforms' strongest signals of customer satisfaction, and are relied upon for a number of purposes, including as a threshold for

115. Airbnb host sign up process [screenshot on file with authors]. *See generally What are References on Airbnb?*, AIRBNB, https://www.airbnb.com/help/article/173/what-are-references-on-airbnb (last visited Mar. 18, 2018).

116. LINKEDIN, *Recommending Someone, LinkedIn Help*, https://www.linkedin.com/help/linkedin/answer/97 (last visited September 6, 2017).

117. LINKEDIN, *Skill Endorsements -- Overview, LinkedIn Help*, https://www.linkedin.com/help/linkedin/answer/31888/skill-endorsements-overview (last visited September 6, 2017).

118. Ruomeng Cui et al., *Discrimination with Incomplete Information in the Sharing Economy: Field Evidence from Airbnb* (Jan. 9, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2882982; *see also* Jun Li et al., *A Better Way to Fight Discrimination in the Sharing Economy*, HARV. BUS. REV. (Feb. 27, 2017), https://hbr.org/2017/02/a-better-way-to-fight-discrimination-in-the-sharing-economy.

119. *Id.*

120. Caroline O'Donovan, *That Four-Star Rating You Left Could Cost Your Uber Driver Her Job*, BUZZFEED (Apr. 11, 2017), https://www.buzzfeed.com/carolineodonovan/the-fault-in-five-stars.

deactivation,[121] an indicator of problematic transactions, or a basis for subsequent sorting, matching, and filtering by users.

Ratings tend to be a coarse form of evaluation; they require the distillation of multifaceted experiences into a discrete value, and are very rarely accompanied by more specific justification or explanation of the rater's source of (dis)satisfaction.[122] Further, rating interfaces seldom include guidelines about what qualities of the interaction a rater ought, or ought not, to consider. For instance, should the rating encompass only the timeliness of a service or the quality of goods delivered? Should it also pertain to the personal interaction between users (i.e., how much the rater liked or felt affinity for the ratee)? This coarseness makes the act of rating a ready conduit for bias to enter into user interactions. As we have described at length elsewhere,[123] there is ample risk that rating processes on platforms may systematically disadvantage marginalized groups, who may receive lower aggregate ratings than other groups; social science research on workplace evaluations finds such effects.[124] In some cases, if platforms make material employment determinations based on consumer-sourced ratings, they may create a facially neutral avenue through which discrimination can creep into employment decisions, despite the fact that a company would be prohibited from making such biased assessments directly.[125]

C. MONITORING AND EVALUATING

Platforms may rely on a diverse set of methods to identify, sanction, and correct for biased behavior among their users. They may create infrastructures through which users can report apparent cases of discrimination that may serve as the basis for sanction. However, such reports can be a way for users to discriminate against one another if users abuse the reporting mechanism to falsely accuse others. Platforms may also take steps to improve the quality of evaluations rendered by users—for instance, by requiring users to submit more granular information in suspect cases, by validating evaluations with independent data sources, or by

121. *See* Rosenblat et al., *supra* note 5.

122. However, some platforms may seek more granular evaluations for particularly poor ratings; *see* Part II.C.2, *infra*.

123. Rosenblat et. al., *supra* note 5.

124. *See, e.g.*, Emilio J. Castilla, *Gender, Race, and Meritocracy in Organizational Careers*, 113 AM. J. SOC. 1479 (2008); Marta Elvira & Robert Town, *The Effects of Race and Worker Productivity on Performance Evaluations*, 40 INDUS. REL. 571 (2001).

125. Rosenblat et. al, *supra* note 5; *see also* Dallan F. Flake, *When Should Employers Be Liable for Factoring Biased Customer Feedback into Employment Decisions?*, 102 MINN. L. REV. __ (Forthcoming 2018).

reweighting evaluations suspected to be influenced by bias. Finally, platforms can measure how certain key outcomes vary according to users' race, gender, and other protected characteristics that they can report publicly or make accessible to regulators and outside researchers. They can also perform controlled experiments or rely on natural experiments to assess whether disparities in outcome owe to differences in these characteristics alone.

1. Reporting and sanctioning

Another set of strategies involves infrastructures for reporting behavior that seems to exhibit bias, and sanctioning users who propagate it. In creating these mechanisms, platforms often take their cues from users who report witnessing or being subject to perceived biased behavior. Such reporting systems are common on social media platforms for marking *explicit* manifestations of bias, offensive content, and overt harassment—often through a flagging system, which may automatically remove content or refer it to a site moderator for review.[126]

Reporting and sanctioning mechanisms have been implemented in attempts to mitigate implicit bias *offline* as well. Complaints to the Equal Employment Opportunity Commission commonly allege that an employer (or prospective employer) behaved in a manner that disproportionately impacted members of a protected class; these complaints act as a trigger for further investigation by the EEOC. A number of colleges and universities have recently launched bias response hotlines and reporting mechanisms aimed at improving campus climate, often including both overt manifestations of bias (e.g., hate speech) as well as implicitly or unintentionally biased behavior.[127]

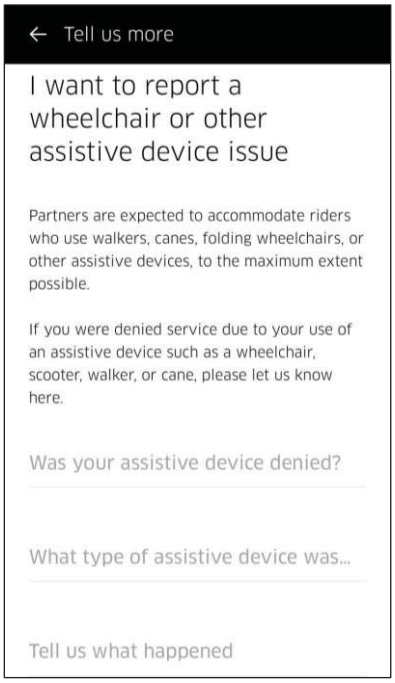
Like these offline analogues, platform bias reporting mechanisms typically elevate concerns institutionally by referring them to a platform

126. *See, e.g.,* J. Nathan Matias et al., *Reporting, Reviewing, and Responding to Harassment on Twitter*, WOMEN, ACTION, AND THE MEDIA REPORT (May 13, 2015), http://womenactionmedia.org/twitter-report; Kate Crawford and Tarleton Gillespie, *What is a Flag For? Social Media Reporting Tools and the Vocabulary of Complaint*, 18 NEW MEDIA & SOC'Y 410, 411 (2016) ("'Flagging'—a mechanism for reporting offensive content to a social media platform—is found on nearly all sites that host user-generated content, including Facebook, Twitter, Vine, Flickr, YouTube, Instagram, and Foursquare, as well as in the comments sections on most blogs and news sites.").

127. At some campuses, such mechanisms have instigated controversy around concerns about their potential chilling effects on academic freedom. *See* Jake New, *Defending BARTs*, INSIDE HIGHER ED (Sep. 12, 2016), https://www.insidehighered.com/news/2016/09/12/despite-recent-criticism-college-officials-say-bias-response-teams-fill-important.

representative or site moderator with authority to adjudicate or investigate the issue. Airbnb's new Open Doors policy, for instance, ensures that guests who report having been unable to find a rental due to discrimination can receive "timely, 24/7, personalized, hands-on support from a specially trained Airbnb employee" who will find the guest a similar listing or an "alternative accommodation option" (presumably, a hotel).[128] Uber riders who report, for instance, a driver's refusal to accommodate a walker or other assistive device can submit a report (see Figure 6); such a report temporarily deactivates the driver account while the company reviews the incident, and confirmed violations of the law may result in the driver's deactivation from the platform.[129]

Figure 6: Uber's mechanism for reporting a driver's refusal to accommodate assistive devices



Systems that rely on users to report manifestations of implicit bias may be difficult to implement in practice. Unlike explicitly discriminatory or harassing conduct, users may lack access to signals that indicate when implicit bias is likely at work or how the design of a platform might

128. Murphy, *supra* note 18, at 21.

129. *Accessibility at Uber*, UBER, https://accessibility.uber.com/#our-policies (last visited September 6, 2017).

exacerbate or mitigate it. Users may have very little insight into how similarly situated users are treated on the platform relative to others; and because they may not interact with the same user on the platform repeatedly, it may be difficult to assess a pattern of behavior (as compared, say, to a managerial relationship in a traditional employment context). In addition, it may be difficult for users to understand what constitutes bias, so that they can usefully report it. Nextdoor, in its attempts to mitigate racial profiling on its platform, initially asked users to flag posts for "racial profiling," a solution that was later deemed inadequate because "many people didn't understand what it was, and Nextdoor members began reporting all kinds of unrelated slights as racial profiling."[130]

In addition, bias reporting systems may *themselves* operate as mechanisms through which bias can be instantiated on a platform. Users may report each other as a means of personal attack, retribution, or to police viewpoints with which they disagree[131]—and different groups of users may be differentially reported on platforms, reducing their ability to participate as part of the community.

Platforms may also sanction users for behavior that appears to exhibit bias *without* reliance on the user community to report it.[132] Airbnb noticed a problem wherein potential guests would attempt to book a listing listed as available, only to be told by hosts that it was not, in fact, vacant for the dates in question—and that those listings were then sometimes booked by guests of a different race.[133] In response, Airbnb changed its platform to automatically prevent a listing from being subsequently booked for a given date if a host tells a potential guest that the space is unavailable. By making it structurally impossible for a host to rebook a space for a "more desirable" guest, Airbnb aims to discourage behavior likely to be inflected with bias.

2. Data quality and validation

Users commonly provide feedback on each other's performance in the course of using a platform—by rating one another, leaving reviews on past transactions, and the like. Though such activity can provide a basis for trust and reliability with unknown partners, it is also likely to be inflected by users' implicit biases and may therefore result in systematically worse

130. Hempel, *supra* note 24.

131. Crawford & Gillespie, *supra* note 126, at 420, 423–24. *See also* our discussion of reporting and transphobia on Tinder, *infra*, footnotes 170–83.

132. *See also infra* Part II.C.2.

133. Murphy, *supra* note 18, at 20.

outcomes for users from marginalized groups.[134] To ameliorate these effects, platforms may seek to improve the quality of evaluations that users tender to one another on a platform. They may do this by requiring more granular information of users in suspect cases, in efforts to make users reflect more precisely on the factors on which their evaluations depend.[135] They may also mitigate the effects of bias (if not bias itself) by adjusting ratings or de-listing reviews likely to be impacted by bias, perhaps using machine learning techniques to detect high- or low-quality evaluations. Finally, platforms may require validation of poor evaluations with external sources of data.

Nextdoor has been the subject of significant controversy in recent years, following media coverage of the platform's users engaging in racial profiling when reporting nearby crimes or suspicious activities.[136] The platform explored a number of strategies to address the problem, ultimately adopting a number of different approaches,[137] including changes to the interface where users report such activity. In particular, Nextdoor now notes when users rely on race to report a crime or suspicious activity,[138] operating under the assumption that such reports are likely to be biased. If this occurs, Nextdoor prompts users to first describe the incident without describing the people involved in the incident. Once users have submitted this information, they are then taken to a second prompt where Nextdoor asks users to fill in predefined fields describing those involved in the incident—and users must fill in at least two of four fields, none of which are related to race (see Figure 7). By forcing users to provide more specific and granular information, Nextdoor limits the degree to which the reporting of crime or suspicious activity can rely solely on the race of the person involved in the incident. While the platform has found that imposing this additional burden seems to discourage users from reporting such events, its leadership believes that it encourages users to think more carefully about the cause of their suspicion and provide more accurate and useful reports.[139]

134. *Id.*

135. Hempel, *supra* note 24.

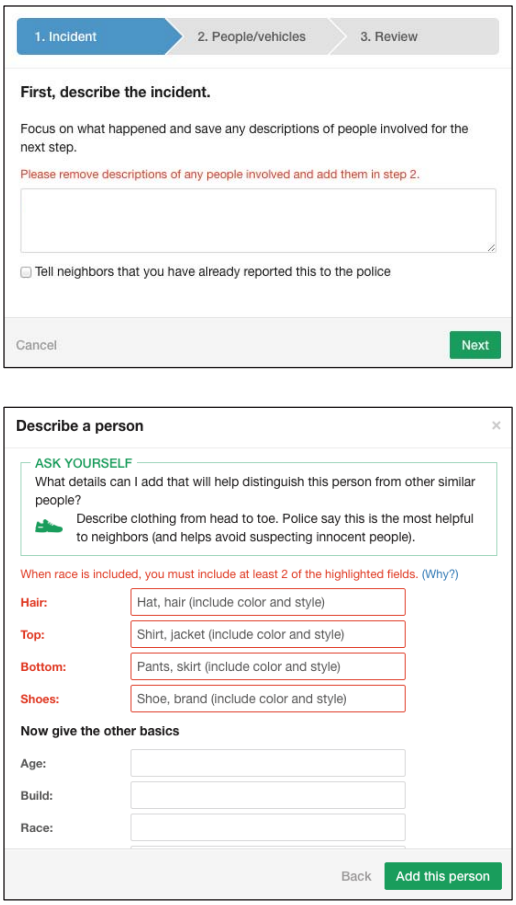
136. Pendarvis Harshaw, *Nextdoor, The Social Network for Neighbors, Is Becoming a Home for Racial Profiling*, FUSION (Mar. 24, 2015), https://fusion.kinja.com/nextdoor-the-social-network-for-neighbors-is-becoming-1793846596.

137. *See infra* Parts II.A.2 and II.B.1.

138. Hempel, *supra* note 24 ("If you refer to race in your description of the incident, Nextdoor's algorithms detect it and prompt you to save this part of the description for the next screen.").

139. *Id.*

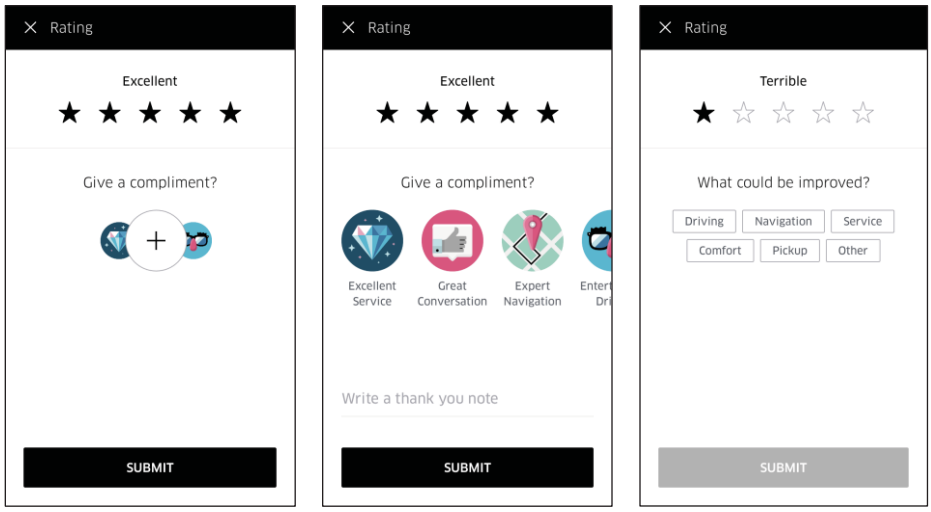
Figure 7: Nextdoor's prompts when users rely on race to report suspicious activity



Uber employs a similar strategy in its rating system, where riders can choose among a set of predetermined and specific compliments to accompany their five-star ratings of drivers, ranging from "Great Conversation" to "Expert Navigation" to "Neat and Tidy". When riders provide ratings lower than five stars, Uber asks "What could be improved?" and provides riders with a set of predefined answers (Comfort, Driving, Navigation, Pickup, Service, and Other) (see Figure 8). While Uber prompts and often requires riders to provide a star rating to drivers, giving a specific compliment is entirely optional. In contrast, Uber may require riders to specify what drivers could have improved when riders give drivers less than five stars. In both cases, Uber seems to want to find a way to solicit more precise and actionable information from riders than the company and drivers might glean from stars on their own. As with Nextdoor, requesting this additional information may impose an additional burden that users

might not always be willing to shoulder, but it can also help to reduce the likelihood that riders are assessing drivers merely on the basis of who the drivers happen to be and not on the quality of their service.[140]

Figure 8: Uber's interface allows riders to give compliments following 5-star ratings, and requires riders to provide suggestions for improvement following 1-star ratings



The quality of users' ratings and reviews can vary dramatically.[141] Some users may invest considerable time and thought in their evaluation while others might pass quick judgment.[142] Less deliberative assessments are likely to be of poorer quality, of course, but also more likely to rely on crass heuristics and thus involve implicit bias. Platforms that rely on users' ratings and reviews tend to be well aware of this problem, and researchers

140. Rosenblat, *supra* note 121.

141. Susan M. Mudambi & David Schuff, *What Makes a Helpful Online Review? A Study of Customer Reviews on Amazon.com*, 34 MGMT. INFO. SYS. Q. 185, 186 (2010); Stefan Siersdorfer et al., *How Useful Are Your Comments?: Analyzing and Predicting YouTube Comments and Comment Ratings*, PROC. ACM INT'L CONF. ON WORLD WIDE WEB 891, 892 (2010).

142. Data quality adjustments are commonly made in related data-collection contexts to guard against manipulation, inattention, and other sources of inaccuracy. Daniel M. Oppenheimer et al., *Instructional Manipulation Checks: Detecting Satisficing to Increase Statistical Power*, 45 J. EXPERIMENTAL SOC. PSYCH. 867, 868 (2009); Chrysanthos Dellarocas, *Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior*, PROC. ACM CONF. ON ELECTRONIC COMMERCE 150 (2000); Andrew Whitby et al., *Filtering Out Unfair Ratings in Bayesian Reputation Systems*, 6 PROC. WORKSHOP ON TRUST IN AGENT SOCIETIES 106 (2004).

have developed a variety of techniques to address it.[143] Yelp, for example, automatically evaluates the quality of users' reviews and prioritizes them accordingly.[144] The platform purposefully does not highlight reviews from new users or users about whom Yelp knows very little; it attempts to weed out reviews from "family, friends, or favored customers" or reviews purchased by the business owner (in an attempt to either benefit the business or hurt a competitor); and it tries to avoid "unhelpful rants and raves," which the company does not define.[145] While many of these reviews remain accessible to interested users, Yelp itself will not factor the scores from these reviews into a business' average score. To the extent that biased assessments are generally more likely to occur in assessments of poor quality, automated systems that aim to remove such reviews and ratings or prioritize high quality evaluations will likely reduce how much bias affects those subject to such evaluations.[146] Yet Yelp's application of such techniques has not been without controversy, in large part because it reveals just how much power it wields in deciding how businesses ultimately fare on its platform.[147]

Adjusting for data quality in terms of removing user *bias* is even more complicated normatively, in that such corrections imply that users' biased judgments are less valid and ought not be considered.[148] Despite this complexity, platforms may still see fit to identify and adjust biased data, to the extent that they can, to diminish the systemic effects of bias on marginalized users. Or they might decide that certain decisions are too consequential to hinge on ratings and reviews from which potential bias

143. *See, e.g.,* Yang Liu et al., *Modeling and Predicting the Helpfulness of Online Reviews*, IEEE INT'L CONF. ON DATA MINING 443 (2008); Dellarocas, *supra* note 142.

144. Yelp, Inc., *How Yelp Helps You Find the Right Local Business*, YELP BLOG (Nov. 13, 2013), https://www.yelpblog.com/2013/11/yelp-recommended-reviews.

145. Yelp stresses that its "recommendation software is entirely automated so that it can apply the same objective standards to every business and every review without being overridden by someone's personal preferences." *Id.*

146. Yelp reviews nevertheless continue to exhibit bias. *See* Sharon Zukin et al., *The Omnivore's Neighborhood? Online Restaurant Reviews, Race, and Gentrification*, J. CONSUMER CULTURE 1 (2015).

147. Jay Barmann, *Yelp is Allowed to Manipulate Ratings and Remove Good Reviews, Says Court*, SFIST (Sep. 4, 2014), http://sfist.com/2014/09/04/yelp_is_allowed_to_manipulate_ratin.php.

148. *See* Rosenblat, *supra* note 5, at 15 ("[t]he suggestion that implicit or explicit consumer biases ought not inflect [user-to-user] ratings … —or at least, that platforms ought to account and correct for the likely presence of such biases—represents a complex normative judgment, and we must acknowledge that adjustments to correct for bias in this context are therefore more normatively laden than adjustments made to correct for systematic error (e.g., sampling bias) in standard data analysis").

cannot be completely purged, in an attempt to limit the effects of biased ratings rather than address the bias itself.[149]

Finally, platforms might rely on alternative sources of information to confirm or validate users' claims. For example, should one user give another a low rating, the platform might ask the initial user to furnish documentary evidence to support broad claims about the quality of the service she received from the other user. Airbnb, for example, might ask the user to photograph any problems with the property. Or the platform itself might try to collect or repurpose data that would allow it to serve as a reliable source against which to judge the validity of users' claims. Uber might examine the location data it collects from riders' phones to see whether they were late to meet their drivers; the data Uber collects from drivers' phones might help to confirm whether they made any unsafe or erratic maneuvers.[150]

While soliciting high quality and informative feedback from users can help to mitigate bias, doing so is not without costs. If platforms ask users to complete more detailed reviews—and therefore spend more time and thought on their assessments—platforms may find that fewer users are willing to even complete the process. If platforms instead attempt to evaluate the quality and reliability of users' assessments and adjust or discount these accordingly, platforms may court controversy by exercising direct control over the relative standing of different users, even if the effect may be to reduce the influence of bias in these users' ratings. And because much of the success of platforms owes to the fact that they have been able to push a good deal of the bureaucracy that comes along with traditional service providers onto users themselves, platforms might balk at the idea of investing the resources necessary to perform user evaluations themselves, even if these might be much less biased than those currently performed by platforms' untrained users.

3. Measurement and detection

Finally, platforms may make independent efforts to measure any potentially disparate effects of their design decisions or to detect bias in the behavior of their users. These approaches draw from offline analogues like the collection of demographic data[151] and the use of audit or correspondence

149. Rosenblat, *supra* note 5.

150. *Id.*

151. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION, *Race/Ethnicity Self-Identification Forms*, https://www.eeoc.gov/employers/eeo1survey/sample_self_identification.cfm (last visited September 6, 2017).

studies in such areas as employment, housing, and credit, among others.[152] Platforms might seek to collect demographic data from their users directly or infer it from other disclosed information.[153] In either case, such details would serve as the necessary foundation to establish whether users from different protected groups fare differently on these platforms, but not whether such differences were the result of biased decision-making.[154] These findings could be reported publicly, much like the transparency reports about government requests for user data that have become common among the major online platforms.[155] As part of these reports, platforms might also describe their methodologies and release the underlying data.[156] In April 2017, California's Department of Fair Employment and Housing entered into a voluntary agreement with Airbnb to resolve the agency's prior complaint against the company for violations of the California Fair Employment and Housing Act and Unruh Civil Rights Act.[157] As part of this agreement, Airbnb assented to generating and sharing such reports with DFEH, noting the average "relative acceptance rate" for users of different races, among other things.[158] The Agreement even suggests that Airbnb

152. Devah Pager & Hana Shepherd, *The Sociology of Discrimination: Racial Discrimination in Employment, Housing, Credit, and Consumer Markets*, 34 ANN. REV. SOC. 181, 184–85 (2008).

153. Platforms might be reluctant to collect this information or attempt to infer it, as users might perceive such activities as a privacy violation or posing risks of discrimination. Separately, users might not want to volunteer demographic information, especially if they are concerned with discrimination.

154. A disparate impact case would start with the same analysis: a showing, for example, that female job, housing, or credit applicants fare systematically worse than male applicants.

155. Laura DeNardis and Andrea M. Hackl, *Internet Governance by Social Media Platforms*, 9 TELECOMM. POL'Y 39, 761–70 (2015). *See also* Aaron Belzer & Nancy Leong, *The New Public Accommodations*, 105 GEO. L.J. 1271, 1319 (2017) (proposing federal legislation to mandate such disclosure by platforms and noting the benefits of providing such data for researchers).

156. Benjamin Edelman, *Response to Airbnb's Report on Discrimination* (Sep. 19, 2016), http://www.benedelman.org/news/091916-1.html ("Certainly Airbnb could provide the interested public with aggregate data measuring discrimination and showing the differential outcomes experienced by white versus black users. If Airbnb now has mechanisms to measure discrimination internally, as the report suggests, it's all the more important that the company explain its approach and detail its methodology and numerical findings—so past outcomes can be compared with future measurements.")

157. California Dep't of Fair Emp. and Housing (DFEH), *Voluntary Agreement between Airbnb and DFEH* (Apr. 19, 2017), https://www.dfeh.ca.gov/files/2017/04/04-19-17-Airbnb-DFEH-Agreement-Signed-DFEH-1-1.pdf.

158. Lyft has adopted a similar approach in response to a letter from former Senator Al Franken, raising concerns about disparate rates at which drivers cancelled rides for black and white passengers. *See* Alan Franken, *Letter to Travis Kalanick and Logan Green* (Nov.

consider creating something functionally akin to transparency reports, but for hosts: a gallery of the guests that hosts have rejected. Such a gallery would act as a kind of mirror through which hosts would be able to take a hard look at their past decisions, possibly revealing patterns of prejudice that would shame hosts or highlighting apparent, but unrecognized, bias that would spur them to alter their behavior. Where guests' races are known, the platform could instead communicate to hosts the relative rates at which they accept guests of different races.

Platforms could also experiment with design choices and observe if they result in any corresponding change in outcomes for minority and marginalized populations. For example, Airbnb has publicly committed to "perform[ing] tests[,]…examin[ing] algorithms, and mak[ing] ongoing adjustments to the technical underpinnings of [its] platform" to explore what might help address the incidence of apparent discrimination. The goal of such experimentation need not be to determine when and where users act in a prejudicial or biased manner; rather, it could simply be to assess whether adjustments to the user experience can help minimize or eliminate disparities in outcomes, regardless of the underlying and ultimate cause of the disparities. Of course, platforms could also experiment to determine which types of interventions are most effective in addressing users' biases more directly. Over a three-month period, Nextdoor tried a number of approaches, which they evaluated through A/B testing, before settling on a final set of strategies.[159] Ray Fisman and Michael Luca have described this as "[maintaining] an experimental mindset," calling on companies that make extensive use of such experimental techniques in product and service development to apply them to the problem of discrimination as well.[160]

Platforms might be more ambitious and attempt to estimate the extent to which bias affects users' decisions by relying on either natural or controlled experiments. In the former, platforms might seek out seemingly

---

2, 2016), https://www.franken.senate.gov/files/letter/161102_UberLyft.pdf. As a means to address the issue, Lyft stated it would enhance its regular review of ride cancellations by "including a focus on cancellation rates and quality of service in 'minority census tracts.'" Logan Green, *Letter in Response to Nov. 2, 2016 Letter to Travis Kalanick and Logan Green* (Dec. 16, 2016), https://www.franken.senate.gov/files/letter/161216LyftResponseLtr.pdf. Franken's letter followed a paper published by the National Bureau of Economic Research establishing patterns of discrimination on both Uber and Lyft in Seattle, WA, and Boston, MA. Yanbo Ge et al., *Racial and Gender Discrimination in Transportation Network Companies* (Nat'l Bureau of Econ. Research, Working Paper. No. w22776, 2016). Many of the paper's recommendations appear directly in Lyft's response to Franken.

159. Hempel, *supra* note 24.

160. Fisman & Luca, *supra* note 1, at 94.

equivalent cases that resulted in different outcomes, where only a difference in race, for example, seems to account for differences in decision-making. In the latter, platforms might devise experiments of their own where they purposefully generate cases that only differ in the race of test users. At the extreme, platforms could even administer psychological tests to directly measure implicit bias among a subset of their users.[161] Armed with the results of these experiments or tests, platforms could then use machine learning to uncover relationships between the more easily observable qualities or behaviors of users and their propensity for biased decision-making. In effect, these platforms would be able to estimate how much bias likely influences each user's decisions. These strategies are not entirely hypothetical: Airbnb has stated publicly that as part of its effort to address discrimination, the platform is exploring how machine learning might "help enforce our anti-discrimination policy."[162]

In addition to taking steps to measure bias and its effects *themselves*, platforms might also take steps to open their data to independent scrutiny by researchers or government entities. A number of social science researchers are interested in conducting studies to detect and measure discrimination on platforms, but often the methods required for doing so are expressly prohibited by a platform's terms of service.[163] Platforms routinely block researchers' accounts when they are suspected of engaging in such research.[164] What's more, researchers who try to detect discrimination on platforms may be subject to criminal penalties; the Computer Fraud and Abuse Act (CFAA)[165] prohibits "unauthorized access" to a computer, which has been interpreted to include terms-of-service violations.[166] Platforms

161. Brian Uzzi, *How Human-Machine Learning Partnerships Can Reduce Unconscious Bias*, ENTREPRENEUR (Jul. 31, 2016), https://www.entrepreneur.com/article/278214.

162. David King, *A Fair Community for Everyone*, AIRBNBCITIZEN (May 11, 2016), https://www.airbnbcitizen.com/a-fair-community-for-everyone/.

163. Christian Sandvig et al., *Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms*, PROC. WORKSHOP ON DATA AND DISCRIMINATION, INTL. COMM. ASSOC. (2014), http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf.

164. *See, e.g.*, Sam Levin, *Airbnb Blocked Discrimination Researcher Over Multiple Accounts*, THE GUARDIAN (Nov. 17, 2016), https://www.theguardian.com/technology/2016/nov/17/airbnb-while-black-discrimination-harvard-researcher-banned.

165. 18 U.S.C. § 1030.

166. The American Civil Liberties Union and several social scientists are currently challenging the constitutionality of the CFAA in light of this issue. *See* Russell Brandom, *New ACLU Lawsuit Takes on the Internet's Most Hated Hacking Law*, THE VERGE (Jun.

might therefore alter their terms of service to permit "bona fide testing"[167] in the service of removing barriers to researchers' detection of bias (for instance, by permitting researchers to operate multiple accounts in order to compare outcomes across race or gender). In addition to facilitating researchers' access, platforms might open their data to scrutiny by government regulators. Airbnb's agreement with the California Department of Fair Employment and Housing requires Airbnb to permit the agency to conduct fair housing testing—essentially, an audit study—through which the agency will set up multiple profiles to discern differential treatment.[168] Under the agreement, Airbnb will further provide the agency with the names of hosts who are suspected of discrimination for testing purposes.[169]

* * *

The ten categories we describe above are ideal types; in practice, platforms' structures are likely to encompass multiple categories. Some features are likely to function in combination—a platform that requests or requires that users disclose particular fields of information about themselves, for instance, may concomitantly allow other users to search and filter by those fields.

But interactions among design features can be more complex as well, with implications for how bias is instantiated on the platform. Consider, for instance, the dating app Tinder's treatment of its transgender users.[170] Tinder's user interface is designed to be minimal and low-friction, such that users simply swipe left or right on each other's profiles to indicate interest in one another, often based on little more information than a profile picture.[171] Until recently, Tinder permitted people to list one of two options for their gender—male or female—without further specification of gender identity; users could specify if they were interested in being matched with

29, 2016), https://www.theverge.com/2016/6/29/12058346/aclu-cfaa-lawsuit-algorithm-research-first-amendment.

167. Benjamin Edelman, *Response to Airbnb's Report on Discrimination* (Sep. 19, 2016), http://www.benedelman.org/news/091916-1.html.

168. California Dep't of Fair Emp. and Housing (DFEH), *Voluntary Agreement between Airbnb and DFEH* (Apr. 19, 2017), https://www.dfeh.ca.gov/files/2017/04/04-19-17-Airbnb-DFEH-Agreement-Signed-DFEH-1-1.pdf, at 16.

169. *Id.* at 17.

170. We gratefully acknowledge Anna Lauren Hoffmann for bringing this example to our attention.

171. Carson Griffith, *On a Phone App Called Tinder, Looks Are Everything*, N.Y. TIMES (Apr. 24, 2013), http://www.nytimes.com/2013/04/25/fashion/on-a-phone-app-called-tinder-looks-are-everything.html.

men, women, or both.[172] As a result, transgender users were often matched with other users who had not realized they had indicated interest in a transgender user. Some users responded to this information negatively, and as a result, reported transgender users (potentially leading to the suspension of their accounts) or subjected them to offensive and abusive language using the app's messaging feature.[173] In order to prevent such abuse, some transgender users took extra steps to make their gender identity as visible as possible in their profile pictures (e.g., by displaying a tote bag reading "PROUD TO BE TRANS");[174] others refrained from using the platform altogether.[175]

The Tinder case demonstrates how design features interact in complicated ways and how addressing bias effectively requires a multi-pronged approach. Here, a limitation on what users reveal about themselves[176] and on how users find one another[177] resulted in abusive reporting[178] that ultimately affected the composition of the community.[179] In response, Tinder eventually made design changes to address this issue, expanding selectable gender options to a list of over 35 suggestions, plus a free-text field, and giving all users the option of whether they want their gender displayed on their profile[180]; however, users cannot yet filter their matches according to these options.[181] In addition, Tinder has engaged in messaging to reframe the norms of the community around diversity and inclusivity (including a campaign around the hashtag #AllTypesAllSwipes),[182] has conducted training for its staff and allocated

172. Megan Rose Dickey, *Tinder Finally Adds Options for Trans and Gender Non-Conforming People*, TECHCRUNCH (Nov. 15, 2016), https://techcrunch.com/2016/11/15/tinder-finally-adds-options-for-trans-and-gender-non-conforming-people/.

173. Madison Malone Kircher, *Transgender People are Reportedly Being Banned from Tinder*, BUSINESS INSIDER (Jun. 3, 2015), http://www.businessinsider.com/transgender-tinder-users-reported-and-banned-2015-6; Addison Rose Vincent, *Does Tinder Have a Transphobia Problem?*, HUFFINGTON POST (Mar. 25, 2016), http://www.huffingtonpost.com/addison-rose-vincent/does-tinder-have-a-transp_b_9528554.html.

174. Vincent, *supra* note 173.

175. Kircher, *supra* note 173.

176. *See supra* Part II.B.3.

177. *See supra* Part II.B.2.

178. *See supra* Part II.C.1.

179. *See supra* Part II.A.2.

180. *See supra* Part II.B.3.

181. Sophie Kleeman, *Tinder Introduces More Inclusive Gender Options*, GIZMODO (Nov. 15, 2016), http://gizmodo.com/tinder-introduces-more-inclusive-gender-options-1788992315.

182. *See supra* Part II.A.3. *See also Introducing More Genders on Tinder*, TINDER BLOG: BEHIND THE SCENES (Nov. 15, 2016), http://blog.gotinder.com/genders/.

additional resources to its support team, and has been working in consultation with gender non-conforming users and representatives from GLAAD.[183]

A naive attempt to addressing bias on platforms—say, one that focuses on a single strategy—might not acknowledge how users' biases, even if thwarted by one feature, can readily migrate to another feature of the platform, and can even lead to abusive encounters.[184] A coherent approach must acknowledge complexities and interactions among platform features, and consider their normative dimensions, which we discuss below.

III. CONCLUSION: ETHICAL DIMENSIONS OF PLATFORM DESIGN

As we have noted, platforms face emergent and uncertain legal obligations in the face of their users' discriminatory behaviors. But even absent legal requirements, platforms may feel an ethical responsibility or public pressure to confront bias exhibited in user-to-user interactions; few platforms want to condone discrimination or develop reputations as bastions of unfair treatment. At the same time, platforms might hesitate to interfere in the business of consenting users, or to identify which of their users seem to exhibit prejudice or bias. Even attempting to minimize the degree to which implicit bias might affect users' decisions raises several normative questions, for which there may be no easy or obvious answers.

First, in the absence of laws that proscribe or prescribe certain behavior, platforms might question whether they possess—or have been granted—the moral authority to decide which types of user preferences are acceptable and which are objectionable, even if they make such decisions unintentionally in developing their products and services. Answering such questions explicitly will require normative principles that can help distinguish cases in which platforms would be wrong to infringe on users' personal autonomy from those in which platforms can override users' preferences in the interest of combating discrimination. In matters of employment, housing, and credit, platforms might feel at ease looking to discrimination law as a source of moral authority and practical guidance in deciding how to regulate the way users can treat one another. In commerce more generally and in more intimate affairs, platforms will have less obvious places to look. In the case of online commerce, platforms might

183. *See supra* Part II.A.1.

184. *See supra* Part II.B.3 (discussing the withholding of user profile photos); *see also infra* note 158 and accompanying text (discussing the relationship between withholding passenger information and low ratings on rideshare sites).

default to a position that leaves users with considerable freedom to contract as they please, even though certain users' preferences might rest on prejudicial or biased beliefs. Indeed, the very point of many platforms' business models is to allow users to choose with whom to transact. Practically, platforms like Craigslist might attempt to compel sellers to accept all comers, but no intervention could force potential buyers to transact with particular sellers. At best, Craigslist might steer potential buyers to a diverse set of sellers; it cannot command potential buyers to do business with these sellers.

Online dating presents an even more charged situation. These platforms are expressly in the business of catering to the preferences of their users, even though they cannot avoid influencing these preferences through their recommendations and other design choices.[185] How platforms should go about influencing these tastes is controversial, to say the least: which predilections should they cultivate and which should they challenge? In particular, should platforms attempt to counteract the tendency toward assortative mating and the preference to date within one's own racial group? Platforms may hesitate to publicly interfere in decisions that users perceive as deeply personal and intimate, preferring, instead, to present themselves as vehicles for satisfying one's predetermined romantic or erotic desires. Moreover, accommodating users' preferences may serve positive ends by shielding people from experiences of prejudice and facilitating efficient matches, as Emens argues: "people's explicit articulation of their dating preferences as to race, (dis)ability, and sex may be efficient for—or even, in some cases, appreciated by—prospective mates (and non-mates). Gays and lesbians, for example, have long understood the utility of creating distinctive spaces for gay socializing; even in the absence of a need to avoid detection or violence, queer-only spaces save time and energy, not to mention needless rejection."[186] In fact, platforms that purposefully limit the efficiency of searches for sexual minorities—by, for example, refusing to provide tools to filter by sexual orientation—may end up discriminating against these populations.[187]

185. *See, e.g.,* Christian Rudder, *We Experiment On Human Beings!*, THE OKCUPID BLOG (Jul. 28, 2014), https://theblog.okcupid.com/we-experiment-on-human-beings-5dd9fe280cd5 (describing how experiments with the information available to Okcupid users affected user interactions).

186. Emens, *supra* note 83, at 1353.

187. *See, e.g.*, *eHarmony, Inc. Settles Class Action Lawsuit over Same-Sex Matching*, BUSINESS WIRE (Jan. 26, 2010), http://www.businesswire.com/news/home/20100126007340/en/eHarmony-Settles-Class-Action-Lawsuit-Same-Sex-Matching (describing the settlement of a lawsuit asserting that the platform had violated state civil rights law by failing to allow users to search for same-sex partners on the site).

Second, platforms might wonder whether they should attempt to limit how easily users can exercise their biased preferences if the platforms cannot prevent users from *holding* such preferences. Specifically, platforms might find that attempts to address bias do not eliminate or diminish bias, but simply push it to other parts of users' interactions where platforms exercise less control or where the bias is less obvious. Ge et al., for example, argue that transportation platforms that deny drivers information about would-be passengers may limit the degree to which drivers can discriminate between requesters, but that prejudiced or biased drivers might nevertheless give certain passengers low ratings, hurting these passengers' abilities to attract even unbiased drivers in the future.[188] In this case, platforms committed to combatting discrimination might allow users to be biased in their choice of a counterparty, if only to ensure that parties unfairly rejected at the outset do not face even greater penalties later in the process or more severe challenges on the platform in the future. Forcing encounters or interactions between users that one or both parties would prefer to avoid may have unintended effects if either party can punish the other in parts of the process over which platforms maintain less effective control.

Finally, because there are few more serious accusations than bias, platforms run considerable risk when they set out to identify bias in their users' behavior. Cultural and political norms are such that almost no one will readily admit to overt prejudice or intentional discrimination, and most will resist claims that their decisions might have been swayed by implicit bias. And yet platforms have begun to explore many ways to uncover just how much their users discriminate against one another. First, they have begun to track differences in users' experience by race, for example, on the belief that such differences must reflect unfair treatment on the platform. Second, some have begun to develop more sophisticated methods to establish the degree to which other users' biases *cause* these differences. And third, some have even committed to using related methods to identify the *specific* users who exhibit these biases. Each can raise very different concerns. In the first case, simply ascribing differences in users' experiences on the platform to bias treats any difference as necessarily suspect and may foster an environment where bias serves as the presumed explanation for any adverse outcome. The corresponding interventions would not be able to target the source of bias and would justify changes to the platform that equalize the experience of users from different racial groups, for example, even if these interventions impose costs and unwelcome changes on others. Platforms that attempt to determine whether

188. Yanbo Ge et al., *supra* note 158, at 20.

bias actually accounts for these differences will fare much better, especially if they do not attempt to pin bias on specific users. Executing such studies will be challenging, however, especially with observational data alone, as platforms rarely have users that resemble each other on every relevant dimension but race, for example, which would be necessary to establish that race explains the difference in outcome. But the dangers are greatest when platforms aim to identify when *specific* users are behaving in a prejudicial or biased manner. Platforms could easily find themselves building models to estimate the extent to which racial bias, for example, influences users' decisions. Discounting, penalizing, or expelling users from the platform on the basis of these inferences, whether in secret or in public, could be highly problematic. Public accusations of bias are very serious, especially should these prove incorrect, but so too are unexplained actions on the part of platforms, driven by suspicions of bias, that shape people's life chances and everyday experience of the world.

As more of the exchanges that comprise daily life—from finding work to finding a date, getting a ride to getting a loan—move online, platforms cannot help but wield great influence over how their users interact. In scaffolding these exchanges, they have no choice but to interact with the biases users bring to the table. Platforms' dominance in so many domains of daily life puts them in a unique position in which they have power to perpetuate, exacerbate, or alleviate its effects in society. As we established in this Article, the levers at platforms' disposal are numerous, and may be mutually reinforcing. Our goal was to highlight the primacy of policy and design in how bias plays out on platforms, to provide a conceptual framework to identify the strategies available to them, and to draw attention to the legal and ethical considerations that adoption of different strategies might entail. Determining the efficacy of these interventions will require further empirical research, and these findings will help platforms to ascertain the most effective solutions for alleviating discrimination.

HOW DIGITAL ASSISTANTS CAN HARM OUR ECONOMY, PRIVACY, AND DEMOCRACY

Maurice E. Stucke[†] *& Ariel Ezrachi* [††]

ABSTRACT

Digital assistants embody the dream of an effortless future, free from the shackles of yesteryear: a tool which caters to users' needs, excels at anticipating their wants, and delivers a personalized online environment. While digital assistants can certainly offer great value, a closer look reveals how—in an algorithm and data–driven world—a dominant digital assistant may ultimately serve the interests of corporations rather than consumers. Such assistants may be used to establish a controlled and manipulated personalized environment in which competition, welfare, privacy, and democracy give way to corporate interests. The future is not necessarily bleak, but requires our attention if users want the leading assistants to match the effortless dream.

DOI: https://doi.org/10.15779/Z383B5W79M

† Professor, University of Tennessee College of Law; Co–founder, The Konkurrenz Group.

†† Slaughter and May Professor of Competition Law, The University of Oxford. Director, Oxford University Centre for Competition Law and Policy.

TABLE OF CONTENTS

I. INTRODUCTION

"All you need to do is say," a 2017 article proclaimed, "'I want a beer' and Alexa will oblige. The future is now."[1] Advances in technology have seemingly increased the choices available to consumers and the convenience of purchasing goods. As sales migrate from brick–and–mortar shops to online sites, consumers appear to be getting more of what they

1. Matt Tate, *Amazon's New Alexa Update Means It Can Bring You Beer in Two Hours*, SHORTLIST (Mar. 21, 2017), http://www.shortlist.com/tech/gadgets/you-can-now-tell-amazons-alexa-to-bring-you-a-beer-amazon-echo.

desire, including better prices and quality. Such a reality may initially appear welcome and desirable. And yet, looking beyond the ease of online shopping, the super–dominant platforms that have emerged pose several growing threats, including algorithmic collusion, behavioral discrimination, and anticompetitive abuses.[2] Thus, a more complex reality exists.

To see why, this Article examines the developing frontier of personal digital assistants. These helpers are being developed by the leading online platforms: Google Assistant, Apple's Siri, Facebook's M, and Amazon's Alexa–powered Echo.[3] These super–platforms are heavily investing to improve their digital assistant offerings.[4] This Article shows how network effects, big data, and big analytics will likely undermine attempts to curtail the digital assistant's power, and will likely allow it to operate below the regulatory and antitrust radar screens. As a result, rather than advancing overall welfare, a dominant digital assistant—if left to its own devices—can undermine our collective welfare. But the harm is not just economic. The potential anticompetitive consequences from a dominant assistant will likely take a toll on privacy, well–being, and democracy.

For those who grew up watching *The Jetsons*, the prospect of a personal helper might seem marvelous. Many already rely on Google's search engine to find relevant results, Facebook to identify relevant news stories, Amazon for book recommendations, and Siri to place phone calls, send text messages, and find a good restaurant nearby. Many also already benefit from basic digital assistants. Apple iPhones users may instruct Siri to call

2. *See generally* ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2016).

3. Alphabet Inc., Annual Report (Form 10-K), at 5 (Feb. 03, 2017) (identifying digital assistant providers "such as Apple, Amazon, Facebook, and Microsoft" as competitors) [hereinafter *Annual Report*]. We will refer to the parent holding company Alphabet as Google. Although Microsoft competes in this arena, it announced in 2017 its plans to allow its voice-enabled digital assistant Cortana to work with Amazon's Alexa. Jay Greene & Laura Stevens, *Amazon's Alexa and Microsoft's Cortana Will Soon Be Able to Talk to Each Other*, WALL ST. J. (Aug. 30, 2017, 3:18 p.m.), https://www.wsj.com/articles/amazons-alexa-and-microsofts-cortana-will-soon-be-able-to-talk-to-each-other-1504120490. Whether this makes Microsoft a stronger or weaker competitor remains to be seen. Finally, Samsung competes in this space as well. Laura Stevens & Tripp Mickle, *Alexa and Siri Escalate Battle of Virtual Assistants*, WALL ST. J. (Sept. 1, 2017 7:09 PM), www.wsj.com/articles/alexa-and-siri-escalate-battle-of-virtual-assistants-1504307382.

4. Solomon Israel, *Why Apple, Amazon, Google and Microsoft Are All Betting on Smart Speakers*, CBC NEWS (June 12, 2017, 5:00 AM), www.cbc.ca/news/business/smart-speakers-apple-amazon-google-microsoft-1.4153237.

their family members on speakerphone.[5] Siri can "predict" what app users might want to use, which music they would like to hear. Navigation apps can anticipate where an individual is heading throughout the day and provide traffic updates and time estimates.[6] Even one's favorite coffee outlet may send a notification and prepare the loyalty card on the device whenever consumers are near an outlet.[7]

Personal digital assistants are also seeking to interact with users in a human–like way. With increasing sophistication, digital assistants promise to transform how individuals access information, communicate, shop, are entertained, control smart household appliances, and raise their children.[8] Digital assistants will also undertake mundane tasks and free up time for users. Amazon's voice recognition personal assistant Alexa, for example, can already perform many tasks. Alexa can shop (knowing everything one previously bought through Amazon); plan one's mornings, including accounting for upcoming meetings, traffic, and weather; entertain one with music; suggest movies, shows, or audiobooks; and control one's smart appliances at home.[9] In 2016, Google showed a video of a suburban family undergoing its morning wakeup routine: "The dad made French press coffee while telling Google to turn on the lights and start playing music in his kids' rooms. The mom asked if 'my package' had shipped. It did, Google said. The daughter asked for help with her Spanish homework."[10] As a digital assistant—powered by sophisticated algorithms—learns more about its users, their routines, desires, and communications, it can excel in its role.[11]

5. *See, e.g.*, Paul Horowitz, *Make a Speakerphone Call with Siri from iPhone*, OSXDAILY (Aug. 1, 2015), http://osxdaily.com/2015/08/01/make-speakerphone-call-siri-iphone/.

6. *See, e.g.*, Lisa Eadicicco, *Google Maps' New Hidden Feature Could Be Very Useful*, TIME (Jan. 13, 2016, 3:24 PM), http://time.com/4178860/google-maps-new-feature/ (describing predictive features of Google Maps application).

7. Sarah Perez, *Starbucks Rolls Out a More Personalized Mobile App Along with a Revamped Rewards Program*, TECHCRUNCH (Apr. 12, 2016), https://techcrunch.com/2016/04/12/starbucks-rolls-out-a-more-personalized-mobile-app-along-with-a-revamped-rewards-program/.

8. EZRACHI & STUCKE, *supra* note 2, at 191–202.

9. Greg Miller, *Amazon Echo: The World's Smartest Assistant*, WALL ST. DAILY (Aug. 4, 2015), http://www.wallstreetdaily.com/2015/08/04/amazon-echo-assistant/.

10. Danny Yadron, *Google Assistant Takes on Amazon and Apple to be the Ultimate Digital Butler*, GUARDIAN (May 18, 2016, 2:17 PM), https://www.theguardian.com/technology/2016/may/18/google-home-assistant-amazon-echo-apple-siri.

11. Ariel Ezrachi & Maurice Stucke, *How Online Competition Affects Offline Democracy*, OXFORD BUS. LAW BLOG (Feb. 16, 2017), https://www.law.ox.ac.uk/business-law-blog/blog/2017/02/how-online-competition-affects-offline-democracy.

In a human–like manner, it can be funny—at just the appropriate level—and trustworthy.[12]

Digital assistants can provide more than information and services; they can anticipate a user's needs and requests.[13] After all, being privy to so many of its users' activities, the assistant will become their digital shadow. As Google's CEO noted, "[y]our phone should proactively bring up the right documents, schedule and map your meetings, let people know if you are late, suggest responses to messages, handle your payments and expenses, etc."[14] The digital assistant, with its users' trust and consent, will likely become the key gateway to the internet.[15] Because of personalization and customization, consumers will likely relinquish other less personal and useful interfaces, and increasingly rely on their digital assistants to anticipate and fulfill their needs.

These technological developments promise to transform and improve the lives of consumers, yet they come at a cost. As they occupy a critical gatekeeper position in a multi–sided market, the assistants may not always operate with consumer interests in mind. This reality raises challenging questions: Despite their apparent promise, can digital assistants actually reduce consumer welfare? Might their rise reduce the number of gateways to the digital world, increase a few firms' market power, and limit competition? And if so, what are the potential social, political, and economic concerns?

Our Article seeks to address these questions. Part II discusses the current race among the super–platforms (Google, Apple, Facebook, and Amazon) to control as many aspects of the online interface as possible and reap the associated benefits. The stakes are high, given several data–driven network effects that will likely lead to market dominance for one or two digital assistants. What are the implications of this winner–take–all contest to be the chief digital assistant? Part III considers the toll a dominant digital assistant can have on competition, democracy, and privacy. Given these risks, one would expect and hope for a "virtuous assistant"—a class of independent assistants, developed by independent firms who treat the users' personal interests as paramount. Part IV identifies several factors that favor

12. *See, e.g.*, Karen Haslam, *Funny Things to Ask Siri*, MACWORLD (July 24, 2017), http://www.macworld.co.uk/feature/iphone/funny-things-ask-siri-3656639/.

13. Ezrachi & Stucke, *supra* note 11.

14. *Google CEO Pichai Sees the End of Computers as Physical Devices*, ECON. TIMES (Apr. 29, 2016, 3:58 PM), http://economictimes.indiatimes.com/tech/internet/google-ceo-pichai-sees-the-end-of-computers-as-physical-devices/articleshow/52040890.cms.

15. *Id.*

one of the four super–platforms capturing the digital assistant market and disfavoring the development of an independent virtuous assistant. As market forces will not necessarily prevent and correct the harms we identify, Part V outlines several issues and challenges confronting antitrust enforcers. Part VI concludes.

II. THE HIGH STAKES RACE AMONG DIGITAL ASSISTANTS

Sales for digital assistants are accelerating, with 35.6 million people in the United States forecasted to use a smart speaker in 2017, up 129% from 2016.[16] Currently Google, Apple, and Amazon are jockeying for their digital assistant to become consumers' chief assistant.[17] Samsung and Microsoft are also in the race, and Facebook is expected to enter with its assistant, "M."[18] With Amazon controlling an estimated 70% of the smart–speaker market as of early 2017—versus 24% for Google Home[19]—the stakes are great and go beyond the mere use of the digital assistant. In this competitive race, each super–platform wants its digital assistant to become the consumers' primary interface—with good reason.

Default options and first–mover advantage matter in the online world.[20] Digital assistants like Alexa, as this Part explores, create a positive feedback

16. Jack Nicas, *Google Gives Artificial Intelligence More Power in Its Products*, WALL ST. J. (May 17, 2017, 6:59 PM), https://www.wsj.com/article_email/google-gives-artificial-intelligence-more-power-in-its-products-1495050967-lMyQjAxMTE3MjE0ODExNjg1Wj/. Alexa–enabled devices, Amazon reported in 2017, "were the top-selling products across all categories on Amazon.com this holiday season. Customers purchased and gifted a record-setting number of devices from the Amazon Echo family with sales up over 9x compared to last holiday season." *Alexa Devices Top Amazon Best-Seller List this Holiday – Millions of Alexa Devices Sold Worldwide*, BUS. WIRE (Dec. 27, 2016, 9:00 AM), http://www.businesswire.com/news/home/20161227005118/en/Alexa-Devices-Top-Amazon-Best-Seller-List-Holiday.

17. Christopher Mims, *Ask M for Help: Facebook Tests New Digital Assistant*, WALL ST. J. (Nov. 9, 2015, 12:00 AM), http://www.wsj.com/articles/ask-m-for-help-facebook-tests-new-digital-assistant-1447045202.

18. Jessi Hempel, *Facebook Launches M, Its Bold Answer to Siri and Cortana*, WIRED (Aug. 26, 2015, 1:00 PM), https://www.wired.com/2015/08/facebook-launches-m-new-kind-virtual-assistant/.

19. Jack Nicas, *Google's New Products Reflect Push into Machine Learning*, WALL ST. J. (May 18, 2016, 11:05 PM), http://www.wsj.com/articles/googles-new-products-reflect-push-into-machine-learning-1463598395.

20. As noted by European Competition Commissioner Margrethe Vestager, "if Google's apps are already on our phones when we buy them, not many of us will go to the trouble of looking for alternatives. And that makes it hard for Google's competitors to persuade us to try their apps." Margrethe Vestager, How Competition Supports Innovation

loop from increasing levels of usage. As more people use a particular digital assistant, the greater the demand for products and services that can connect to that digital platform, the more likely other manufacturers and developers will develop applications for that platform, and the more appealing the platform becomes to consumers, manufacturers, and software developers.[21]

A. NETWORK EFFECTS: WHERE THE BIG CAN GET EVEN BIGGER

"Network effects occur when the value of a product or service for a customer increases when the number of other customers also using it increases."[22] A telephone is a classic example. As more people have a telephone, the more people one can call, the more use one gets from one's phone. Facebook's social network and navigation apps illustrate these network effects. While network effects may be beneficial, they may also tilt the market in favor of a given provider or technology. The stakes are significant with digital assistants because at least four data–driven network effects are at play.

(May 24, 2016), https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/how-competition-supports-innovation_en; *see also* Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECH. L.J. (forthcoming 2017); J. Jonas Anderson, *Secret Inventions*, 26 BERKELEY TECH. L.J. 917, 956 (2011) ("[F]irst-mover advantage . . . serves as an alternate means of recouping initial investments"); Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible*, 24 BERKELEY TECH. L.J. 1133, 1152 n.85 (2009) (describing related conditions when first–mover advantages are most useful); Stuart J.H. Graham, Robert P. Merges, Pam Samuelson & Ted Sichelman, *High Technology Entrepreneurs and the Patent System: Results of the 2008 Berkeley Patent Survey*, 24 BERKELEY TECH. L.J. 1255, 1289 (2009) (explaining that first–mover advantage was "clearly ranked the most important" goal for patent holders in large–scale study of patent holder motivations).

21. *See, e.g.*, Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1010 (2016) (explaining that "[i]ndirect network effects" occur because "the more widely end users adopt a company's platform, the more vendors and developers are drawn to the platform and vice versa" such that "a company that eventually owns the dominant platform will obtain a tremendous monopoly advantage"); Rambus v. F.T.C. *in the Context of Standard-Setting Organizations, Antitrust, and the Patent Hold-Up Problem*, 24 BERKELEY TECH. L.J. 661, 663, 665 (2009) (describing the analogous problem of technology lock–in as a similar anticompetitive problem).

22. Commission Decision No. M.8124 (Microsoft/LinkedIn), ¶ 341 (Dec. 6, 2016) [hereinafter *Microsoft/LinkedIn Decision*], http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf; *see also* United States v. Microsoft, 253 F.3d 34, 49 (D.C. Cir. 2001).

1. Attracting Manufacturers and Developers

One network effect is the positive feedback loop in attracting manufacturers and developers.[23] It will likely be inefficient for developers to create apps, hardware, and software for every digital assistant.[24] Instead they likely will focus on the top–selling digital assistants.[25] So, if more people primarily use Amazon's Alexa, its operating platform's applications and functions will likely attract more developers and smart appliance manufacturers. Consequently, Alexa will learn more skills relative to competitors, making it more attractive than rival digital assistants.

This feedback loop has already begun to manifest in the market. In 2015, to increase sales of Alexa, Amazon opened its Alexa Voice Service to third–party hardware makers, "giving them the tools to integrate Alexa into internet-connected devices."[26] The aim was to connect Alexa to more

---

23. Indirect network effects arise when people increasingly use a product or technology (for example, software platforms). *See* Virginia E. Scholtes, *The* Lexmark *Test for False Advertising Standing: When Two Prongs Don't Make a Right*, 30 BERKELEY TECH. L.J. 1023, 1025 n.10, 1056 (2015). The more people that use the platform, "the more there will be invested in developing products compatible with that platform, which, in turn reinforces the popularity of that platform with users." Case T-201/04, Microsoft Corp. v. Comm'n, 2007 E.C.R. II-3601, ¶1061.

24. United States v. Microsoft Corp., 84 F. Supp. 2d 9, 20 (D.D.C. 1999):

> The fixed costs of producing software, including applications, is very high. By contrast, marginal costs are very low. Moreover, the costs of developing software are "sunk"—once expended to develop software, resources so devoted cannot be used for another purpose. The result of economies of scale and sunk costs is that application developers seek to sell as many copies of their applications as possible. An application that is written for one PC operating system will operate on another PC operating system only if it is ported to that system, and porting applications is both time-consuming and expensive. Therefore, application developers tend to write first to the operating system with the most users—Windows. Developers might then port their applications to other operating systems, but only to the extent that the marginal added sales justify the cost of porting. In order to recover that cost, ISVs that do go to the effort of porting frequently set the price of ported applications considerably higher than that of the original versions written for Windows.

25. Marina Lao, *Reclaiming A Role for Intent Evidence in Monopolization Analysis*, 54 AM. U. L. REV. 151, 184 (2004) ("To attract users, any new OS system must support at least all the popular software applications, but few software developers are willing to write applications for a system that does not have a large 'installed base,' i.e., users.").

26. Patrick Nixon, *Bezos: Mexico Launch Is Amazon Highlight in Q2*, BUS. NEWS AM. (July 24, 2015), http://www.bnamericas.com/en/news/ict/fri-bezos-mexico-launch-is-amazon-highlight-in-q2.

"smart" appliances, like lights, fans, switches, thermostats, garage doors, sprinklers, locks, and other devices. Amazon announced in early 2017 that "[t]ens of thousands of developers" were using the Alexa Voice Service to integrate Alexa into their products, including "Dish DVRs, Ford and Volkswagen vehicles, GE C Lamp, Huawei Mate 9, LG Smart Instaview fridge, and Whirlpool appliances."[27] Thus, as more people use Alexa, more manufacturers will make smart–products which Alexa can control, and the more appealing Alexa becomes to prospective purchasers and manufacturers.

A second feedback loop occurs as developers teach the digital assistant new skills. Amazon, for example, offers a free Alexa Skills Kit, which "makes it fast and easy for developers to create new voice-driven capabilities for Alexa."[28] As more people purchase Alexa, more companies will develop new skills for Alexa. In early 2016, for example, Alexa could directly order a pizza from Domino's or a car from Uber, check credit card balances with Capital One, get fitness information from Fitbit, offer election updates from NBC News, play Jeopardy!, get stock quotes with Fidelity, hear headlines from the Huffington Post, provide a seven–minute workout, and test trivia knowledge with quizzes from Disney.[29] Indeed, Alexa's skills selection tripled in three months in 2016 alone, with over "3,000 skills available, including Food Network, GE Appliances, Yahoo Sports Fantasy Football, and more."[30] By mid–2016, Amazon had "tens of thousands of developers building new skills for Alexa."[31] Also in 2016 Amazon announced "the Alexa Prize, an annual university competition with $2.5 million dedicated to accelerating the field of conversational artificial intelligence."[32] The competition's aim is "to build a 'socialbot' on Alexa

27. *Amazon.com Announces Fourth Quarter Sales up 22% to $43.7 Billion*, BUS. WIRE (Feb. 02, 2017, 4:01 PM) http://www.businesswire.com/news/home/20170202006227/en/Amazon.com-Announces-Fourth-Quarter-Sales-22-43.7.

28. David Isbitski, *Introducing the Alexa Skills Kit, Enabling Developers to Create Entirely New Voice Driven Capabilities*, AMAZON DEVELOPER BLOG (June 25, 2015), https://developer.amazon.com/blogs/post/Tx205N9U1UD338H/Introducing-the-Alexa-Skills-Kit-Enabling-Developers-to-Create-Entirely-New-Voic.

29. *Amazon.com Announces First Quarter Sales up 28% to $29.1 Billion*, BUS. WIRE (Apr. 28, 2016, 4:01 PM), http://www.businesswire.com/news/home/20160428006852/en/Amazon.com-Announces-Quarter-Sales-28-29.1-Billion.

30. *Amazon.com Announces Third Quarter Sales up 29% to $32.7 Billion*, BUS. WIRE (Oct. 27, 2017, 4:01 PM), http://www.businesswire.com/news/home/20161027006743/en/Amazon.com-Announces-Quarter-Sales-29-32.7-Billion.

31. *Id.*

32. *Id.*

that will converse with people about popular topics and news events."[33] Thus, as more people use a particular digital assistant, more companies will develop new skills for that digital assistant (like ordering beer and pizza), which makes the digital assistant more appealing to prospective purchasers and developers.

This type of network effect helped Microsoft maintain its dominance in personal computer operating systems for decades. In *United States v. Microsoft Corp.*, the government argued that network effects acted as structural barriers for those seeking to enter the market for Intel–compatible personal computer operating systems.[34] The U.S. Court of Appeals agreed, and held that an "applications barrier to entry" protected Microsoft's dominance.[35] That barrier resulted because "(1) most consumers prefer operating systems for which a large number of applications have already been written; and (2) most developers prefer to write for operating systems that already have a substantial consumer base."[36] This "chicken-and-egg" situation "ensures that applications will continue to be written for the already dominant Windows, which in turn ensures that consumers will continue to prefer it over other operating systems."[37] The court also noted that this applications barrier to entry led consumers to prefer the dominant operating system, even if they did not need all the available applications:

> The consumer wants an operating system that runs not only types of applications that he knows he will want to use, but also those types in which he might develop an interest later. Also, the consumer knows that if he chooses an operating system with enough demand to support multiple applications in each product category, he will be less likely to find himself straitened later by having to use an application whose features disappoint him. Finally, the average user knows that, generally speaking, applications improve through successive versions. He thus wants an operating system for which successive generations of his favorite applications will be released—promptly at that. The fact that a vastly larger number of applications are written for Windows than for other PC operating systems attracts consumers

33. *Id.*
34. United States v. Microsoft, 253 F.3d 34, 49–50, 55 (D.C. Cir. 2001).
35. *Id.* at 55.
36. *Id.*
37. *Id.*

> to Windows, because it reassures them that their interests will be met as long as they use Microsoft's product.[38]

This network effect also helped solidify Google's and Apple's dominance over the mobile phone operating system.[39]

2. Learning–by–Doing

Besides this traditional network effect, an additional network effect involves learning–by–doing. Search engines demonstrate this data–driven network effect clearly.[40] Each person's utility from using the search engine increases when others use it as well.[41] As more people use the search engine, the more likely the search engine can learn consumers' preferences, the more relevant the search results will likely be, which in turn will likely attract others to use the search engine; and the positive feedback continues.[42] Interestingly with this network effect, as more people use the service or product, its quality improves.[43]

This learning–by–doing network effect has multiple applications with digital assistants. One is voice recognition. The more people talk to the assistant, the better able the assistant can learn the different pronunciations, sentence structures, and different ways commands can be made.[44] As the algorithm's skill improves in understanding what people want, developers do not have to code for every variation.[45] As Microsoft states, "[w]hether

38. *Id.*

39. Jonathan Sallet, *The Creation of Value: The Value Circle and Evolving Market Structures*, 11 J. ON TELECOMM. & HIGH TECH. L. 185, 234 (2013).

40. MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 172–81 (1st ed. 2016); Press Release, European Comm'n, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 27, 2017), http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm [hereinafter *EC Fact Sheet*] (discussing high barriers to entry in these markets, in part because of network effects: "the data a search engine gathers about consumers can in turn be used to improve results").

41. STUCKE & GRUNES, *supra* note 40, at 170–81.

42. *Id.*

43. *Id.*

44. *Cortana Dev Center*, MICROSOFT, https://developer.microsoft.com/en-us/Cortana (last visited Oct. 24, 2017).

45. This process is called machine learning. *See, e.g.*, *id.*; Christian Chessman, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 181 n.9 (2017) (explaining that machine learning involves combining "rules of analysis" and "repeated exposure to data patterns" in order to iteratively modify software "output or behaviors" over time); M. I. Jordan & T. M. Mitchell, *Machine Learning: Trends, Perspectives, and Prospects*, 349 SCIENCE 255, 255 (2015) ("Machine

someone says 'I need a taxi' or 'call me a cab,'" its digital assistant Cortana "gets it."[46]

A second application occurs when the digital assistant learns relevant responses. For example, one 2017 study compared how Google's and Amazon's digital assistants understood and responded to 800 queries.[47] Both assistants understood approximately 94% of the queries.[48] What is remarkable is that their ability to answer correctly improved significantly between February and August 2017: from approximately 34% to 54% for Amazon and from 39% to 65% for Google.[49] As one reviewer in early 2016 noted, "[w]ith a rapidly growing slate of features, integrations and use cases, it's easy to get excited about the Echo's potential. . . . More than two years after its debut, the smarter-than-ever Amazon remains one of the best connected home products money can currently buy."[50] Over the next few years, as more skills are developed, more features are added, and more trial–and–error learning occurs,[51] digital assistants will be even smarter and in many more homes.[52]

---

learning addresses the question of how to build computers that improve automatically through experience.").

46. MICROSOFT, *supra* note 44; Harry Shum, *Microsoft AI*, MICROSOFT, https://wuncontentservice.blob.core.windows.net/berlin-cms/2017/09/Microsoft-AI-Amplifying-human-ingenuity.pdf (last visited Oct. 24, 2017).

47. Gene Munster, *Faceoff: Amazon Echo Show vs Google Home Part II*, LOUP VENTURES (Aug. 11, 2017), http://loupventures.com/faceoff-amazon-echo-show-vs-google-home-part-ii/.

48. *Id.*

49. *Id.*

50. Ry Crist & David Carnoy, *Amazon Echo Review: The Smart Speaker That Can Control Your Whole House*, CNET (July 18, 2017), https://www.cnet.com/products/amazon-echo-review/.

51. *See infra* Part IV (describing digital assistant learning process).

52. Jim Marous, *Banking Needs An 'Amazon Prime' Marketing Strategy*, FIN. BRAND (July 27, 2017), https://thefinancialbrand.com/66545/amazon-prime-digital-banking-loyalty-experience-strategy/; Mary Branscombe, *Making Cortana Smarter: How Machine Learning Is Becoming More Dynamic*, TECHRADAR (Mar. 19, 2015), www.techradar.com/news/world-of-tech/making-cortana-smarter-how-machine-learning-is-becoming-more-dynamic-1287936; *Google Assistant to Take Over Apple Siri, Amazon Alexa, and Samsung Bixby by 2021: Report*, BGR (Sept. 4, 2017, 2:31 PM), http://www.bgr.in/news/google-assistant-to-take-over-apple-siri-amazon-alexa-and-samsung-bixby-by-2021-report/; Stephen Shankland, *How Apple Uses AI To Make Siri Sound More Human*, CNET (Aug. 23, 2017, 3:17 PM), https://www.cnet.com/news/apple-ai-machine-learning-makes-siri-sound-human-on-ios-11/.

3. Scope of Data

A third data–driven network effect involves the scope of personal data collected, which can be used to personalize tasks and predict individualized user needs. The super–platforms already expend significant effort to better track individuals, collect their personal data, and profile them.[53] So the feedback loop adds another dimension: digital assistants no longer merely rely on aggregated insights from the earlier queries of other users, but instead include an additional layer of insight in predicting individual tastes and preferences by using the variety of personal data the super–platform collects about its users.

In other words, the more one uses a digital assistant, and the more personal data it collects, the more opportunities the digital assistant can anticipate one's particular needs. Super–platforms already expressly recognize this fact; as Microsoft noted, "[w]ith a user's permission, Cortana can deliver unique, personal experiences based on her knowledge of user preferences: everything from their favorite food to the location of their next meeting."[54] The scope of the personal data—"what app you are in, previous search history, your current GPS, as well as personal details"—can also provide the needed context for its user's voice inquiry or in anticipating the user's requests.[55]

As the digital assistant seamlessly converses with users, it can also recognize the household's different voices. So if the mother of a large family asks, "Okay Google, what's on my calendar today?" the digital assistant can identify the speaker.

4. Spill–Over Effects

Because the personal assistant is ostensibly "free" to use, its provider has to monetize its services. One way is through personal data, which it can sell. Or the platform can monetize through advertising and fees from sellers. Here network effects on the "free" (consumer) side can spill over to the "paid" (provider) side, and each side can reinforce the other. As more users with heterogeneous requests are attracted to the digital assistant, a greater variety of advertisers and sellers will migrate to the digital assistant's platform as well.

53. EZRACHI & STUCKE, *supra* note 2, at chs. 15, 16.

54. MICROSOFT, *supra* note 44.

55. Tich Savanhu, *Leveraging the Rise of Voice Search*, BIZCOMMUNITY (Apr. 4, 2017), http://www.bizcommunity.com/Article/196/179/160034.html.

As discussed above, growth in user base for a particular personal assistant will likely drive more companies to develop skills and applications for that assistant.[56] The more consumers rely on a particular digital assistant, the more sellers will be attracted to that platform. The super–platform's power accordingly increases, including the fees it can collect from sellers to transact with its digital assistant's users.[57] (Amazon, for example, earns fees from third–party sellers that sell on its platform.[58]) A dominant platform can also use the inflow of personal data to better target consumers with its own and third–party products and services.

The more personal data the platform collects, the better the platform can target users with personalized sponsored search results and ads.[59] Platforms compete for advertisers based on the return on investment that the platform can deliver.[60] Some of the super–platforms, like Google, earn most of their revenues from advertising.[61] When consumers click on a relevant sponsored ad (which generates revenue on a cost–per–click basis) or see a display ad (which generates revenue on a cost–per–impression basis), Google gets paid.[62] As more users are drawn to the digital assistant and the super–platform's other free services, the super–platform amasses a greater variety of data to effectively target consumers with relevant ads, products, and

56. *See supra* notes 21–24 and accompanying text.

57. *EC Fact Sheet*, *supra* note 40 (discussing how "the more consumers use a search engine, the more attractive it becomes to advertisers" and the "profits generated can then be used to attract even more consumers").

58. *See* Alistair Barr, *Amazon's Sellers Are Furious Over the Website's Fees*, HUFFINGTON POST (May 18, 2013), http://www.huffingtonpost.com/2013/03/18/amazon-sellers_n_2899568.html.

59. Julia Angwin, Surya Mattu & Terry Parris Jr., *Facebook Doesn't Tell Users Everything It Really Knows About Them*, PROPUBLICA (Dec. 27, 2016, 9:00 AM), https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them; Julia Angwin, Madeleine Varner & Ariana Tobin, *Facebook Enabled Advertisers to Reach 'Jew Haters'*, PROPUBLICA (Sept. 14, 2017, 4:00 PM), https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters; Alex Kantrowitz, *Google Allowed Advertisers to Target People Searching Racist Phrases*, BUZZFEED NEWS (Sept. 15, 2017, 11:15 AM), www.buzzfeed.com/alexkantrowitz/google-allowed-advertisers-to-target-jewish-parasite-black .

60. Barr, *supra* note 58; United States v. Bazaarvoice, Inc., No. 13-CV-00133-WHO, 2014 WL 203966, at *21 (N.D. Cal. Jan. 8, 2014) ("A critical asset in building a successful social commerce network is to have the largest audience possible because that is how advertisers and marketers and brands think about the value they get.") (internal quotations omitted).

61. STUCKE & GRUNES, *supra* note 40, at 196–97.

62. *Id.*

services.[63] The more time users spend on the platform's services (such as search engines, email, maps, videos, etc.), the more opportunities the platform can target users in the moments that matter for a purchasing decision, and the more ad revenues it attracts relative to other online sites. This network effect is already at play in online markets; in the first quarter of 2016, for example, it was estimated that "85 cents of every new dollar spent in online advertising" went to Google or Facebook.[64]

Digital assistants are already deploying ads and are likely to continue doing so in the future. In 2017, users of Google's digital assistant received an ad for the movie "Beauty and the Beast" even when they simply asked, "OK Google, what's my day like?"[65] (Google denied calling it a commercial; instead it wanted to "call out timely content."[66]) Amazon is currently testing ads with its digital assistant, and ads are expected to increase.[67] But the ad may not always appear through the digital assistant. A user might ask Google Home about good hotels in Palm Beach, and an advertisement for the Ritz Carlton might appear across its expanding platform of "free" services (such as sponsored search results, ads in emails, and display ads in videos). The ad might also appear across media (such as personal computers, smartphones, tablets, and soon, "smart" household appliances and driverless cars).[68]

Ultimately, as more people use a particular digital assistant, the more skills the assistant acquires, the better the assistant becomes in recognizing commands and faces, the better the assistant becomes in anticipating users' needs and responding to their requests. The platform, in turn, becomes more attractive to sellers and advertisers who want to target these users, which

63. *Id.*

64. John Herrman, *Media Websites Battle Faltering Ad Revenue and Traffic*, N.Y. TIMES (Apr. 17, 2016), https://www.nytimes.com/2016/04/18/business/media-websites-battle-falteringad-revenue-and-traffic.html.

65. Ben Fox Rubin, *Ads for Voice Assistants Are Here and They're Already Terrible*, CNET (Apr. 21, 2017, 5:00 AM), https://www.cnet.com/news/ads-voice-assistants-amazon-alexa-google-home-burger-king/.

66. *Id.*

67. Nicholas Shields, *Get Ready for Ads on Alexa*, BUS. INSIDER (May 15, 2017, 9:33 AM), http://www.businessinsider.com/amazon-trials-voice-assistant-ads-2017-5.

68. Victor Luckerson, *Google Wants to Put Ads in Your Refrigerator*, TIME (May 21, 2014, 12:53 PM), http://time.com/107593/google-ads-nest-refrigerator-internet-of-things/ (noting Google's expectation "that users will be using [its] services and viewing [its] ads on an increasingly wide diversity of devices in the future, and thus [its] advertising systems are becoming increasingly device-agnostic"); *see also* Lothar Determann & Bruce Perens, *Open Cars*, 32 BERKELEY TECH. L.J. 913, 918–19 (2017) (describing "behavioral data" that smart car developers "can monetize for advertising and other purposes").

generates more revenue for the platform to connect its assistant with other technologies and ostensibly "free" services.

B. HOW THE NETWORK EFFECTS INCREASE THE COMPETITIVE STAKES

Firms compete to dominate markets characterized by network effects.[69] As one product or standard increases in popularity, it trends toward dominance. The big get bigger, until they dominate the industry.[70] As one U.S. court observed, "once dominance is achieved, threats come largely from outside the dominated market, because the degree of dominance of such a market tends to become so extreme."[71] At that stage, the benefits from network effects may be dwarfed by the impact on competition and innovation.

Digital assistants are starting to exhibit these network effects. By July 2017, for example, Amazon's Alexa acquired over 15,000 skills—up from its 10,000 skills in February 2017, which was triple what it had in September 2016.[72] By mid–2017, Google in contrast had 378 skills, while Microsoft had only 65 skills.[73] To avoid falling behind, Google is partnering with Walmart Stores Inc. whereby users of Google Express shopping service can easily order from the retail giant using Google's virtual assistant.[74]

As the digital economy shifts from a mobile–dominated world to an AI–dominated platform, the leading platforms' plans are clear: they "envision a future where humans do less thinking when it comes to the small decisions that make up daily life."[75] That increased reliance on the digital assistant is the Holy Grail for the super–platforms. Their aim is to increase the time users spend on their platform—on the gate which they control—which in turn delivers income from advertisements, referrals, and purchasing activities.

The key is to control as many aspects of the online interface and reap the associated benefits. As Google CEO Sundar Pichai wrote shareholders in 2016, "[t]he next big step will be for the very concept of the 'device' to fade away. Over time, the computer itself—whatever its form factor—will

69. Poudel, *supra* note 21, at 1010.
70. *Id.*
71. Novell, Inc. v. Microsoft Corp., 505 F.3d 302, 308 (4th Cir. 2007).
72. Sarah Perez, *Amazon's Alexa Passes 15,000 Skills, Up From 10,000 in February*, TECHCRUNCH (July 3, 2017), https://techcrunch.com/2017/07/03/amazons-alexa-passes-15000-skills-up-from-10000-in-february/.
73. *Id.*
74. Stevens & Mickle, *supra* note 3.
75. Yadron, *supra* note 10.

be an intelligent assistant helping you through your day."[76] Google, for example, announced in 2017 that its Assistant "will soon be available via an app on iPhones . . . as well as a variety of other devices, including refrigerators, washing machines and toys," following a similar move by Amazon.[77] In discussing its digital assistant, Google's CEO said, "We want users to have an ongoing two-way dialogue with Google."[78] Google is not alone in that sentiment; "Alexa may be Amazon's most loved invention yet — literally — with over 250,000 marriage proposals from customers and counting," said Jeff Bezos, Amazon's founder and CEO. "And she's just getting better. Because Alexa's brain is in the cloud, we can easily and continuously add to her capabilities and make her more useful — wait until you see some of the surprises the team is working on now."[79]

As consumers spend more time conversing primarily with their digital assistant, who will increasingly predict and fulfill their needs, they will less frequently search the web, look at price–comparison websites, or download apps. Google's search engine used "to show just ten blue links in [its] results, which you had to click through to find your answers."[80] Now Google is "increasingly able to provide direct answers—even if you're speaking your question using Voice Search—which makes it quicker, easier and more natural to find what you're looking for."[81] Rather than searching online for information, you can now talk with Google Assistant "in a natural conversational way to help you get things done."[82] Thus, Google Assistant forms part of the company's "effort to further entrench itself in users' daily lives by answering users' queries directly rather than pointing them to other sources."[83]

The more a user converses with and delegates to the digital assistant, the better it can predict the user's tastes, and the more likely consumers generally will rely on it for daily activities. As the digital assistant accumulates information over time, the switching costs (and quality gap)

76. Jay Greene, *Microsoft, Other Tech Giants Race to Develop Machine Intelligence*, WALL ST. J. (June 14, 2016, 6:58 PM), http://www.wsj.com/articles/tech-giants-race-to-develop-machine-intelligence-1465941959.

77. Nicas, *supra* note 16.

78. Jack Nicas, *Google Makes Push into Artificial Intelligence with New Offerings*, WALL ST. J. (May 18, 2016, 3:58 PM), https://www.wsj.com/articles/google-makes-push-into-artificial-intelligence-with-new-offerings-1463595169.

79. *Id.*

80. *Annual Report*, *supra* note 3.

81. *Id.*

82. *Id.*

83. Nicas, *supra* note 19.

between digital assistants will become higher.[84] One could therefore be willingly locked into one's comfort zone. Illustrative are efforts by Facebook, which in 2015 announced a beta version of its digital assistant: M.[85] M can replace most web searches and apps with a function within Facebook Messenger.[86] As the next Part discusses, the removal of the human element from the search activity, and partly from the decision–making, transfers more power to the platform. The digital assistant will use its own tools and may exercise its own judgment (or the judgment of the super–platform) as to prioritizing and communicating the results. When it does so, it will not likely have its users' interests in mind.

III. IMPLICATIONS OF THIS WINNER–TAKE–ALL CONTEST TO BE THE CHIEF DIGITAL ASSISTANT

If firms compete to dominate markets characterized by network effects, what are the implications if one or two digital assistants control the market? As this Part explores, a dominant digital assistant may abuse its gatekeeper position in three ways. First, such a digital assistant can lessen competition, to the detriment of sellers upstream and consumers downstream. Second, it poses significant risks to democracy and the marketplace of ideas. Third, it may take a significant toll on privacy and personal peace of mind.

A. ECONOMIC CONCERNS

A dominant digital assistant raises several economic concerns. As illustrated earlier, Google and other super–platforms have the goal of increasingly providing direct answers—through voice queries—which makes it quicker, easier, and more natural to find results. Rather than searching online for information, users will talk with Google Assistant, Alexa, or another digital assistant in a natural and conversational way. By controlling the interface between the user and sellers or advertisers, the companies controlling the dominant digital assistants can abuse their significant market power, adversely affecting both sellers upstream and users downstream.

84. *See, e.g.*, Sharon D. Nelson & John W. Simek, *Are Alexa and Her Friends Safe for Office Use?*, LAW PRAC., September/October 2017, at 27 ("Unfortunately, Amazon uses all of the history to make Alexa 'smarter' by learning what you ask for and how you ask it. If you delete all the voice history, Alexa will effectively revert back to a new factory setting. That's the tradeoff between privacy and usability. Maintaining your privacy means less usability.").

85. Mims, *supra* note 17.

86. *Id.*

1. Upstream Anticompetitive Effects

Consider the following question: who pays the digital assistant? Consumers pay for the hardware, such as for the iPhone to access Siri. But none of the super–platforms charge a monthly fee for using their digital assistants. Once a consumer buys Amazon's Echo, she can access Alexa without additional charges. This initially appears to be extraordinary: each super–platform encourages users to heap as many tasks as possible on its free digital assistant. To contextualize both the invasiveness and magnitude of these digital assistants, consider their analogue: if a company offered you a *human* assistant, upon whom you could heap as many tasks as possible, without incurring any charge, would you accept the offer? Would you trust them with your intimate information, or to observe you in your home? Would you be confident in that assistant to ultimately promote your interests or the company's?

The issue concerns the true employers/principals of these digital assistants. On a superficial level, the digital assistants directly serve users. The digital assistant will dim the lights upon command and change the temperature as needed. But this new trusted alter ego, to whom individuals outsource their decision–making is also partial. After all, being the ostensibly "free" part of a multi–sided market, users do not directly pay for the digital assistant's services. The digital assistant ultimately must cater to the needs of its real employer—the platform. Of course, consumers can still benefit when the platform's interests are aligned with the interests of its users. But individuals may often be unaware of when such alignment is absent.

As more customers rely on the digital assistant for purchases, entertainment, news, services, and information, the more attractive the platform becomes to sellers. Sellers know that the inclusion of their products and services on a platform's search results may be crucial for commercial visibility. As these "information and referral junctions" become a crucial gatekeeper between suppliers and consumers, the platform's bargaining power and ability to distort competition upstream increase.[87]

87. *See, e.g.*, Ioannis Lianos & Evgenia Motchenkova, *Market Dominance and Search Quality in the Search Engine Market*, 9 J. COMPETITION L. & ECON. 419, 422 (2013) ("Search engines act as 'information gatekeepers': they not only provide information on what can be found on the web (equivalent to yellow pages), but they also are 'an essential first-point-of-call for anyone venturing onto the Internet'" and how search engines differ from other two-sided platforms, as they "detain an important amount of information about their customers and advertisers (the 'map of commerce').").

The gatekeeper may charge, like powerful price comparison websites, an entrance fee (commission) from sellers for the right to be featured in the digital assistant's options. Some platforms, for instance, allow for preferential placement based on the level of payment or commission they receive from sellers. For instance, pay–for–placement fees allow a platform to charge higher rates to sellers for the right to be positioned at the top of the list on the default page result. Such positioning may distort competition when the user is unaware of the preferential positioning and assumes that the top results are the best (or most relevant) ones objectively picked by the website's algorithms. One example of such manipulation of results is in online air and hotel bookings.[88] Following Expedia's 2015 acquisition of Orbitz, for example, "the online travel agency implemented a new program that enables hotel properties to move to the first page of Expedia's listings for an additional 10 percent commission."[89] Another example is gas and electricity aggregators.[90] Such aggregators may also delist sellers which are

88. *See, e.g.*, US Airways, Inc. v. Sabre Holdings Corp., No. 11 CIV. 2725 (LGS), 2017 WL 1064709, at *5 (S.D.N.Y. Mar. 21, 2017) ("Ultimately, US Airways had no choice but to accept them in the US Airways-Sabre 2006 contract for fear of being removed from the Sabre GDS or being retaliated against, for example, through 'display biasing,' which means reordering search results as they appear in the system to disadvantage a particular airline."). Several factors can influence how hotel booking intermediaries order hotels, including "customer ratings and complaints"; "if hotels are willing to pay larger commissions"; "photo quality"; and "if a hotel is quicker to turn shoppers into buyers." Scott McCartney, *How Booking Sites Influence Which Hotels You Pick*, WALL ST. J. (Jan. 27, 2016), http://www.wsj.com/articles/how-booking-sites-influence-which-hotels-you-pick-1453921300. Some hotels have criticized how these intermediaries tailor their search results. The American Hotel & Lodging Association told the *Wall Street Journal,* "[b]iased or misleading search results from these sites or via web searches can be highly problematic, particularly on those booking websites that purport to be helping consumers comparison shop based off of less than objective information." *Id.* (internal quotation marks omitted).

89. *Vista/Cvent: High Combined Market Share and Entry Barriers in Strategic Meeting Management Could Create Hurdle to Clearance; Increased DOJ Interest in Data Privacy May Drive Additional Scrutiny*, CAPITOL FORUM (July 20, 2016), http://createsend.com/t/j-2C8274378D0F467C.

90. Rachel Rickard Straus, *Price Comparison Website Bosses Under Attack From MPs for Not Showing Customers the Best Deals*, THIS IS MONEY (Feb. 4, 2014, 6:44 AM), http://www.thisismoney.co.uk/money/bills/article-2939364/Price-comparison-website-bosses-attack-MPs.html ("The executives at uSwitch, MoneySupermarket, Compare the Market, Confused.com and Go Compare were hauled in front of the MPs after it was claimed . . . that some were 'hiding' the best gas and electricity deals from their customers."). Among other things, platforms were accused of "not showing the cheapest tariffs by default if it meant they wouldn't earn a commission." *Id.*

disruptive to the platform's operation (or advertising–driven business model).[91]

Such strategy may further intensify in markets in which the gatekeeper is vertically integrated. For instance, the platform could insist that sellers and buyers use its payment system or other related products.[92] Such integration might enable the gatekeeper to leverage its power to related markets, pushing out independent operators.

Google showed how a powerful intermediary could abuse its market power upstream. Google's search engine is dominant.[93] In 2017, the European Commission fined Google a record amount (€2.42 billion) for abusing its dominant position in searches.[94] As the Commission noted, Google's search engine "provides search results to consumers, who pay for the service with their data."[95] In 2004 Google entered a separate market, namely comparison shopping. One problem for Google was that the comparison shopping market already had several established players; another problem was that Google's product (Froogle) was subpar.[96] But comparison shopping services relied to a large extent on traffic to be competitive.[97] Moreover, the comparison shopping service market has its own network effects: as more customers use that comparison shopping site, the more likely retailers will want to list their products with that comparison shopping service. To improve its position on the market for comparison shopping, Google used its dominant search engine to redirect traffic. From 2008, Google began pushing its own comparison shopping service, while

91. EZRACHI & STUCKE, *supra* note 2, at 179–86.

92. *See, e.g.*, Kathleen De Vere, *Google Tweaks Policy, All Google Play Apps Must Use Google's Payment System*, ADWEEK (July 31, 2012), http://www.adweek.com/digital/google-drops-the-hammer-on-third-party-android-billing-services-apps-must-use-googles-billing-system/.

93. *Search Engine Market Share Worldwide*, STATCOUNTER, http://gs.statcounter.com/search-engine-market-share/all/worldwide/2016 (last visited Oct. 24, 2017) (noting that Google possessed 91.84% search engine market share worldwide in 2016); Press Release, European Comm'n, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 27, 2017), http://europa.eu/rapid/press-release_IP-17-1784_en.htm.

94. Press Release, *supra* note 93.

95. *Id.*

96. *Id.* ("Contemporary evidence from Google shows that the company was aware that Froogle's market performance was relatively poor (one internal document from 2006 stated 'Froogle simply doesn't work').").

97. *Id.* ("More traffic leads to more clicks and generates revenue.").

relegating the rival (and superior) comparison shopping services.[98] Most people click on the first few results provided by Google's search engine.[99] Few people go to the second page, and even fewer go to the third page of results.[100] Google systematically placed its own comparison shopping service on the first page at or near the top of the search results.[101] Google relegated the rival shopping services to later pages—the better ones only appeared on page four of Google's search results, and others appeared even further down the list.[102]

As a result of its illegal practices, Google effectively increased the traffic to its own comparison shopping service, while drying up the traffic to its rivals' services.[103] As the Commission noted:

> Since the beginning of each abuse, Google's comparison shopping service has increased its traffic 45-fold in the United Kingdom, 35-fold in Germany, 19-fold in France, 29-fold in the Netherlands, 17-fold in Spain and 14-fold in Italy. Following the demotions applied by Google, traffic to rival comparison shopping services on the other hand dropped significantly. For example, the Commission found specific evidence of sudden drops of traffic to certain rival websites of 85% in the United Kingdom, up to 92% in Germany and 80% in France. These sudden drops could also not be explained by other factors. Some competitors have adapted and managed to recover some traffic but never in full.[104]

It is remarkable how effectively Google stifled competition in the comparison shopping market. Even though Google was intentionally degrading the quality of its search results, few consumers, if any, switched to other search engines, such as Yahoo! or Bing.[105] Even though competitors were a click away, competition was not. Moreover, users could have scrolled to the fourth page of Google's search results, but few did. For search results on personal computers:

> [T]he ten highest-ranking generic search results on page 1 together generally receive approximately 95% of all clicks on generic search results (with the top search result receiving about 35% of

98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*
105. *Id.* (noting Google's consistently high market share for search in the EU).

> all the clicks). The first result on page 2 of Google's search results receives only about 1% of all clicks. The effects on mobile devices are even more pronounced given the much smaller screen size.[106]

In what consumers often view as a neutral environment, the ability to switch did not match the incentive to do so. Google effectively increased the friction for consumers to use rival shopping services, while reducing the friction for its own (subpar) product.[107]

The anticompetitive effects of search degradation will be likelier and more severe with a dominant digital assistant. For one thing, with the Google Shopping case the issue was whether the rivals' services were on the first, fourth, or subsequent pages of Google's results.[108] In contrast, digital assistants will not provide several pages of results. As they promise to become "more conversational,"[109] digital assistants will likely offer one or two suggestions. If many consumers—whether on their PCs or mobile phones—did not look at the second or third page of the search engine's results, users will likely hear even fewer suggestions from their digital assistant. Moreover, if many users did not "multi–home" by running the same search query on multiple search engines, they are less likely to multi–home by searching independently online. Instead, they will likely rely on their assistant's one or two suggestions.

For example, one 2017 study sought to better understand how Amazon's digital assistant recommends items. Over 450 products—in health care, beauty, household cleaning, electronics, and grocery categories—were ordered, and "an overwhelming number of products Alexa suggested tended

106. *EC Fact Sheet*, *supra* note 40; *see also* ORG. FOR ECON. COOPERATION & DEV., ALGORITHMS AND COLLUSION - NOTE FROM THE UNITED KINGDOM 5 (2017), https://one.oecd.org/document/DAF/COMP/WD(2017)19/en/pdf [hereinafter UK SUBMISSION] ("[H]igh ranking and prominent visibility in search results (whether organic or non-organic) may be important to a business' ability to compete effectively; and this is partly due to consumers' online search behaviours, in particular their propensity to focus their attention, clicks and purchases on links at the top of returned search results and rarely venture beyond the first results page.").

107. Press Release, *supra* note 93.

108. *EC Fact Sheet*, *supra* note 40 ("Real-world consumer behaviour, surveys and eye-tracking studies demonstrate that consumers generally click far more on search results at or near the top of the first search results page than on results lower down the first page, or on subsequent pages, where rival comparison shopping services were most often found after demotion.").

109. Frederic Lardinois, *The Google Assistant Is Getting More Conversational*, TECHCRUNCH (May 17, 2017), https://techcrunch.com/2017/05/17/the-google-assistant-is-getting-more-conversational/.

to be those available to Prime members" and "products with Amazon Choice designation, which is given to the top brand in each product group, were far more likely to be recommended for first-time orders."[110] Thus Alexa did not provide a panoply of products, but recommended ones Amazon specifically designated. And Amazon will not necessarily offer the cheapest or best value product. ProPublica, for example:

> looked at 250 frequently purchased products over several weeks to see which ones were selected for the most prominent placement on Amazon's virtual shelves — the so-called 'buy box' that pops up first as a suggested purchase. About three-quarters of the time, Amazon placed its own products and those of companies that pay for its services in that position even when there were substantially cheaper offers available from others. That turns out to be an important edge. Most Amazon shoppers end up clicking "add to cart" for the offer highlighted in the buy box.[111]

Thus, companies may pay Amazon for this "Choice designation."[112] Or Amazon may simply have its assistant promote its own products.[113]

Another reason why search bias will be likelier and more effective with digital assistants is that it will be harder to detect. In the Google Shopping case, the Commission had a ready counterfactual: namely how the results would have looked if Google's own comparison shopping service were subject to Google's own generic search algorithm.[114] Absent Google's manipulation of the search results, its generic algorithm presumably would have given greater prominence to other shopping services. For example, a rival service might have been on the first page, while Google's shopping service appeared on the fourth page. Thus, the Commission ordered equal treatment, namely that "Google has to apply the same processes and methods to position and display rival comparison shopping services in

110. Marty Swant, *Alexa Is More Likely to Recommend Amazon Prime Products, According to New Research*, ADWEEK (July 7, 2017), http://www.adweek.com/digital/alexa-is-more-likely-to-recommend-amazon-prime-products-according-to-new-research/.

111. Julia Angwin & Surya Mattu, *Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't*, PROPUBLICA (Sept. 20, 2016, 8:00 AM), www.propublica.org/article/amazon-says-it-puts-customers-first-but-its-pricing-algorithm-doesnt.

112. OLIVIA LAVECCHIA & STACY MITCHELL, AMAZON'S STRANGLEHOLD: HOW THE COMPANY'S TIGHTENING GRIP IS STIFLING COMPETITION, ERODING JOBS, AND THREATENING COMMUNITIES 20–21 (2016), https://ilsr.org/wp-content/uploads/2016/11/ILSR_AmazonReport_final.pdf.

113. *Id.* at 24–25.

114. Press Release, *supra* note 93.

Google's search results pages as it gives to its own comparison shopping service."[115]

With digital assistants, the antitrust agency may lack a ready counterfactual, as there might not be a generic search algorithm. Instead, the digital assistant, using the consumer's personal data, personalizes results for that person's tastes. Google Assistant, for example, can utilize users' search history and customize its responses based on what it knows about the users' queries.[116] So when you ask your Assistant, "What movie do you recommend?," your results will likely differ from your neighbor's. Thus, it will be harder for the competition authority to reconstruct what the digital assistant would have recommended, but for the search degradation.[117]

A third reason why search bias will be likelier and more effective with dominant digital assistants is their omnipresence. In the Shopping case, Google could lessen competition even though users could download apps of competing services (or change their default search engine). When many users rely on a dominant digital assistant, it will be harder for the disfavored seller to reach the user. Even when a disfavored seller can gain a user's attention, the digital assistant may interject with its own recommendation, suggesting a special deal by a member of its platform's ecosystem. In this multi–sided market, the digital assistant may subtly push certain products and services and degrade or conceal others, all in the name of personalization. Rather than deter such abuses, market forces, given the data–driven network effects, can actually increase entry barriers.[118]

2. Downstream Anticompetitive Effects

Competition officials are familiar with price discrimination, where different consumers are charged different prices, depending on their willingness and ability to pay. Digital assistants can help facilitate

115. *EC Fact Sheet*, *supra* note 40.

116. *Virtual Assistant Comparison: Cortana, Google Assistant, Siri, Alexa, Bixby*, DIG. TRENDS (Aug. 29, 2017, 8:44 AM), https://www.digitaltrends.com/computing/cortana-vs-siri-vs-google-now/.

117. *Not So Froogle: The European Commission Levies a Huge Fine on Google*, ECONOMIST (July 1, 2017), https://www.economist.com/news/business/21724436-its-case-not-perfect-it-asks-right-questions-european-commission-levies-huge ("If search algorithms become more personalised, as is expected to be the case with digital assistants such as Amazon's Alexa, it will be even more difficult to detect bias.").

118. *EC Fact Sheet*, *supra* note 40 (discussing how network effects increase entry barriers).

behavioral discrimination, a durable, more pernicious form of price discrimination.

Online behavioral discrimination, as we explore in *Virtual Competition*,[119] will likely differ from the price discrimination in the brick–and–mortar world in several important respects. First is the shift from imperfect price discrimination to near perfect, or first–degree, price discrimination. Second, sellers can use the personal data to target consumers with the right emotional pitch to increase overall consumption.[120] A third way behavioral discrimination differs from price discrimination is its durability.

The U.K. competition authority already found price discrimination to be more prevalent online.[121] With a powerful digital assistant, behavioral discrimination becomes likelier. The digital assistant can help the super–platform refine its profile of users, including their likely reservation price (defined as the upper threshold of willingness to pay), use of outside options, shopping habits, general interests, and weaknesses (including moments when their willpower is fatigued).

First, with more personal data about its users' preferences, habits, weaknesses, and other traits, the digital assistant can segment users into even smaller groups to better identify their likely reservation price.[122] The

119. *See generally* EZRACHI & STUCKE, *supra* note 2.

120. Basically, this process involves manipulating personal data in order to get users to purchase items they otherwise did not want, at the highest price they are willing to pay. *See* Ariel Ezrachi & Maurice E. Stucke, *The Rise of Behavioural Discrimination*, 37 EUR. COMPETITION L. REV. 485, 486 (2016).

121. UK SUBMISSION, *supra* note 106, at 7.

122. *Id.* at 2. The United Kingdom noted that:

> Algorithms can be used to set different prices for different customers, including through online tracking and profiling of consumers. The combination of: a) the greater and greater volume of data available to firms about customers, and b) the increasingly sophisticated means of using algorithms to swiftly analyse this data and gather very granular intelligence about customers' preferences, purchases or price sensitivity, is likely to increase further the opportunities for firms to engage in detailed segmentation and price discrimination.

Id. Similarly, Commissioner Terrell McSweeny of the Federal Trade Commission explained:

> Big data and algorithms enable sellers to more effectively target and price discriminate against specific customers. Thus, even though a

ride–sharing app, Uber, for example, confirmed in 2017 that it uses customer data to better price discriminate. As *Bloomberg* reported:

> The new fare system is called "route-based pricing," and it charges customers based on what it predicts they're willing to pay. It's a break from the past, when Uber calculated fares using a combination of mileage, time and multipliers based on geographic demand. Daniel Graf, Uber's head of product, said the company applies machine-learning techniques to estimate how much groups of customers are willing to shell out for a ride. Uber calculates riders' propensity for paying a higher price for a particular route at a certain time of day. For instance, someone traveling from a wealthy neighborhood to another tony spot might be asked to pay more than another person heading to a poorer part of town, even if demand, traffic and distance are the same.[123]

Given its ubiquity in the home, a digital assistant will have even more personal data, more opportunities to observe how users respond to different advertisements, pricing, and products, and more opportunities to learn the right price point for that user. VIZIO, as Section III.C discusses, collected TV data to help third parties analyze a household's behavior across devices. Likewise, a digital assistant, connected to the user's smart television and search engine, can also monitor whether the user visited a particular website following a television advertisement related to that website, or whether the user viewed a particular television program following exposure to an online advertisement for that program.

But the digital assistant could also be proactive. It can recommend the entertainment (such as Alexa suggesting a movie produced or distributed by Amazon), choose the advertisements before the movie, suggest an easy, frictionless way to buy the advertised product ("Alexa, order me this

---

> company may not have been able to effectively target certain consumers for higher prices in the past, that in itself is no guarantee that it might not be able to do so in the future. Data is becoming more robust and algorithms are becoming more powerful. The Commission defined markets on the basis of price discrimination in its successful challenge to the Sysco/U.S. Foods merger — and I would not be surprised to see the concept of price discrimination markets take on increasing importance in U.S. antitrust agency challenges going forward.

Terrell McSweeny, Commissioner, Fed. Trade Comm'n, Competition Law: Keeping Pace in a Digital Age *8 (Apr. 15, 2016), 2016 WL 1613290.

123. Eric Newcomer, *Uber Starts Charging What It Thinks You're Willing to Pay*, BLOOMBERG (May 19, 2017, 12:19 PM), https://www.bloomberg.com/news/articles/2017-05-19/uber-s-future-may-rely-on-predicting-how-much-you-re-willing-to-pay.

product"), deliver quickly that product (through Amazon Prime), and if perishable, remind the user to replenish that product.

Second, as users increasingly converse with and trust it, the digital assistant can learn what emotional pitch will likely induce the user to buy products or services that they might not otherwise have wanted.[124] Facebook, according to an internal document, promoted advertising campaigns that exploited its users' emotional states, including users as young as fourteen years old:

> [T]he selling point of this 2017 document is that Facebook's algorithms can determine, and allow advertisers to pinpoint, "moments when young people need a confidence boost." If that phrase isn't clear enough, Facebook's document offers a litany of teen emotional states that the company claims it can estimate based on how teens use the service, including "worthless," "insecure," "defeated," "anxious," "silly," "useless," "stupid," "overwhelmed," "stressed," and "a failure." . . . [T]he documents also reveal a particular interest in helping advertisers target moments in which young users are interested in "looking good and body confidence" or "working out and losing weight."[125]

Facebook denied offering tools to target people based on their emotional state.[126] Nonetheless, the dark side of behavioral economics emerges. The dominant digital assistant can use the findings from behavioral economics to advance the platform's own interest. As observed in 2011 by an executive of DraftFCB, one of the leaders in thinking about how to incorporate the discipline of behavioral economics with the practice and business of modern advertising and marketing:

> If anything, behavioral economics impact will only grow in the future, because it works hand in glove with the growing centrality of digital solutions in marketing. You can't understand the success of digital platforms like Amazon, Facebook, Farmville, Nike Plus,

124. Ezrachi & Stucke, *supra* note 120.

125. Sam Machkovech, *Report: Facebook Helped Advertisers Target Teens Who Feel "Worthless"*, ARS TECHNICA (May 1, 2017, 12:00 AM), https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/; Nick Whigham, *Leaked Document Reveals Facebook Conducted Research to Target Emotionally Vulnerable and Insecure Youth*, NEWS.COM.AU (May 1, 2017, 2:16 PM), www.news.com.au/technology/online/social/leaked-document-reveals-facebook-conducted-research-to-target-emotionally-vulnerable-and-insecure-youth/news-story/d256f850be6b1c8a21aec6e32dae16fd.

126. *Comments on Research and Ad Targeting*, FACEBOOK (Apr. 30, 2017), https://newsroom.fb.com/news/h/comments-on-research-and-ad-targeting/.

> and Groupon if you don't understand behavioral economic principles like social proof, the impact of variable intermittent social rewards, feedback loops, and scarcity. Behavioral economics will increasingly be providing the behavioral insight that drives digital strategy.[127]

Just as Uber uses the findings from behavioral economics to nudge its drivers,[128] so too the digital assistant can reward users for expanding its role in their daily lives. The digital assistant—in taking on additional tasks—can nudge users along the path of least resistance, offering an array of new rewards for their efforts. Companies are already training algorithms to help them identify human emotions.[129] Affectiva, for example, collected over one billion video frames of facial expressions.[130] Its algorithms, according to its promotional video, can help develop ads that "optimize" a target audience's moment–by–moment engagement and predict likely sales and "virality."[131] Thus, a digital assistant could use "emotion data" to help create content and advertisements to spur consumption.[132]

A third way a dominant digital assistant can facilitate behavioral discrimination is by reducing user exposure to—and incentive to seek—outside options. Friction is the buzzword for online sellers.[133] Amazon is designing its digital assistant to reduce friction—whether in renting a movie

127. John Kenny et al., *Where is Behavioral Economics Headed in the World of Marketing?*, NUDGE BLOG (Oct. 9, 2011), http://nudges.org/2011/10/09/where-is-behavioral-economics-headed-in-the-marketing-worlding/.

128. Noam Scheiber, *How Uber Uses Psychological Tricks to Push Its Drivers' Buttons*, N.Y. TIMES (Apr. 2, 2017), https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html.

129. Luke Dormehl, *AI Assistants Will Soon Recognize and Respond to the Emotion in Your Voice*, DIG. TRENDS (Sept. 14, 2017, 11:41 AM), https://www.digitaltrends.com/cool-tech/affectiva-emotion-in-voice/; Hope Reese, *The Machine Knows How You Feel: How AI Can Detect Emotion*, TECHREPUBLIC (Jan. 4, 2016, 7:44 AM), www.techrepublic.com/article/the-machine-knows-how-you-feel-how-ai-can-detect-emotion/.

130. Dormehl, *supra* note 129; Affectiva, *Affectiva Overview*, YOUTUBE (Nov. 6, 2014), https://www.youtube.com/watch?time_continue=162&v=mFrSFMnskI4.

131. Affectiva, *supra* note 130.

132. Scholars have already begun to consider the practical implications of collecting and monetizing "emotion data" in the analogous context of autonomous cars, which will likely be among the technologies to integrate digital assistants. *See* Determann & Perenz, *supra* note 68, at 920 ("Chemical sensors can detect alcohol and perhaps other chemicals on the breath. If a[n autonomous] vehicle carries such medical sensors, the vehicle–connected computer might also use the data from them to assess whether the driver and passengers are hungry and monetize that as an advertising opportunity.").

133. Marous, *supra* note 52.

or buying more batteries.[134] For example, users of Amazon's digital assistant can sign up for Amazon Prime simply by saying, "Alexa, sign me up for Prime."[135] Once users are signed up, friction is further reduced for verbally ordering items or streaming music. An Amazon executive identified the following questions developers should ask:

- How many decisions are between a customer and completing a task?
- Are each of these decisions absolutely necessary?
- If so, can you make the decision for the customer by pre-selecting an option?
- If not, and the customer absolutely needs to make that decision, how can you simplify the decision process?
- If there are multiple decisions, could you combine them into one decision?
- Can you present the most important decision first to the customer?
- How can you preserve the decision once it's been made so that you don't have to ask the customer again in the future?[136]

A digital assistant's voice activation will reduce friction further. Amazon's digital assistant added in 2017 Alexa Show, where users can easily request, see, and order items from Amazon.[137] Indeed, while Alexa Show looks like a tablet, users primarily converse with it. The greater the ease in conversing with the digital assistant, the less friction in ordering products and services, the more likely users will rely on the digital assistant's recommendations (rather than turning to their PC or phone to search for, and order, products). The company comScore predicts that voice searches will make up fifty percent of all searches by 2020.[138]

---

134. *Id.*

135. *Alexa, What Are Your Prime Day Deals?*, BUS. WIRE (July 5, 2017, 3:42 AM), http://www.businesswire.com/news/home/20170705005339/en/.

136. *Amazon's Friction-Killing Tactics to Make Products More Seamless*, FIRST ROUND REVIEW, http://firstround.com/review/amazons-friction-killing-tactics-to-make-products-more-seamless/ (last visited Oct. 24, 201).

137. WIRED, *Amazon's Alexa Can Now Show You Things | WIRED*, YOUTUBE (June 26, 2017), https://www.youtube.com/watch?v=4TvL8gY-TLQ.

138. Eric Enge, *The Rise of Personal Assistants*, SEARCH ENGINE LAND (Sept. 12, 2017, 9:49 AM), http://searchengineland.com/rise-personal-assistants-280658.

This reduction in friction has already increased sales. Amazon Echo owners in 2016, for example, spent about ten percent more on Amazon than they did before owning the digital assistant.[139] They also purchased from Amazon six percent more often than they did before the digital assistant.[140] According to one press report, "Echo owners may become some of the most valuable customers to Amazon by repeatedly returning to the marketplace and making higher average order values, driving up incremental sales gains for the company."[141] (Likewise, as noted above, Google is coordinating with Walmart so that users can receive personalized shopping results based on their online and in–store Walmart purchases.[142])

As with search degradation, personalization will make behavioral discrimination harder to detect. As a digital assistant learns to accommodate a particular user's particular tastes, it will be harder to identify when the digital assistant degrades quality. "As companies collect more user data and algorithms have more opportunities to experiment (such as presenting items and suggesting other purchases)," the OECD noted, "pricing becomes more dynamic, differentiated and personalised."[143] As more online retailers switch to dynamic (and personalized) pricing and product offerings, it will be harder for consumers to discover a general market price and to assess their outside options.[144] It may be easier to assess quality degradation for objective queries (such as the distance between two cities or the current temperature). But for these objective queries, the digital assistant typically lacks the incentive to intentionally distort quality. After all, its platform will

139. *Amazon Echo Owners Are Spending More Money on Amazon*, BUS. INSIDER (Sept. 19, 2016, 11:30 PM), http://www.businessinsider.com/amazon-echo-owners-are-spending-more-money-on-amazon-2016-9; Darrell Etherington, *Amazon Echo Owners Spend More on Amazon, Says NPD*, TECHCRUNCH (Sept. 15, 2016), https://techcrunch.com/2016/09/15/amazon-echo-owners-spend-more-on-amazon-says-npd/.

140. BUS. INSIDER, *supra* note 139; Etherington, *supra* note 139.

141. BUS. INSIDER, *supra* note 139.

142. Sridhar Ramaswamy, *Shop Walmart and More of Your Favorite Stores, Faster*, GOOGLE (Aug. 23, 2017), https://www.blog.google/products/assistant/shop-walmart-and-more-your-favorite-stores-faster/ ("For example, if you order Tide PODS or Gatorade, your Google Assistant will let you know which size and type you previously ordered from Walmart, making it easy for you to buy the right product again.").

143. ORG. FOR ECON. COOPERATION & DEV., ALGORITHMS AND COLLUSION - BACKGROUND NOTE BY THE SECRETARIAT (2017), https://one.oecd.org/document/DAF/COMP(2017)4/en/pdf [hereinafter OECD BACKGROUND NOTE].

144. Kathy Kristof, *How Amazon Uses "Surge Pricing," Just Like Uber*, CBS NEWS: MONEYWATCH (July 24, 2017, 10:08 AM), https://www.cbsnews.com/news/amazon-surge-pricing-are-you-getting-ripped-off-small-business/.

not profit by telling users it is twenty–eight degrees Celsius, when it is actually twenty–six degrees outside. The danger lies in more subjective queries (or tasks that the digital assistant undertakes automatically).

As a result, digital assistants will blur the line between personalization and behavioral discrimination. Even when users swim upstream by searching the web, the ads, products, or search results they see may be orchestrated by the dominant digital assistant. Consequently, as the assistant accumulates more information, it will be aware of the extent to which users venture out and seek other options. Its aim is to deliver the right product or service at a price that the user is willing to pay. As users increasingly rely on their popular digital assistant for suggestions, it can increasingly suggest personalized things (such as on–demand customized clothing[145]) or services to buy, and the price it has successfully negotiated. As Google noted in 2017, "[s]ometimes your Assistant should be the one to start [the conversation]—so over the next few months, we're bringing proactive notifications to Google Home."[146] While helping one's son with his Spanish, the digital assistant might suggest a particular app or private tutor that tremendously helped other students struggling with the same issue. Because the tutoring is customized, it will be harder to assess whether the price the tutor charges is the fair market price or simply a price its parents would tolerate. Moreover, if the tutoring service is helping other children improve their grades, the parents would not want their child to be at a competitive disadvantage—especially if they eye the same highly selective universities. Thus, the dominant digital assistant can prompt purchases that its users otherwise would not consider, at higher prices, even when competition is a click away.

B. CONCERNS OVER HOW ECONOMIC POWER CAN TRANSLATE INTO POLITICAL POWER

The previous Section illustrated how a dominant digital assistant can confer its provider with market power—namely the ability to command supra–competitive profits through behavioral discrimination, fees on sellers seeking to access users, or search degradation. Importantly, the power does not stop there. As users increasingly rely on the digital assistant, the super–

145. Andrew Tarantola, *Adidas Will Knit You a $200 Sweater While You Wait*, ENGADGET (Mar. 21, 2017), https://www.engadget.com/2017/03/21/adidas-will-knit-you-a-200-sweater-while-you-wait/.

146. Scott Huffman, *Your Google Assistant is Getting Better Across Devices, from Google Home to Your Phone*, GOOGLE (May 17, 2017), https://www.blog.google/products/assistant/your-assistant-getting-better-on-google-home-and-your-phone/.

platform can affect not only what users buy, but also their views and the public debate. The reliance on a powerful gatekeeper could enable its operator to intellectually capture users, and subsequently decision makers, in an attempt to ultimately ensure that public opinion and government policies align with the corporate agenda. While such propositions may sound apocalyptic, they should not be brushed aside.[147] Here we briefly illustrate several risks that a dominant digital assistant could pose to the marketplace of ideas.

One risk is bias. Currently, the super–platforms do not report the news. But many people rely on the super–platforms' algorithms to find news of interest. [148] One concern is that users will prefer news that supports their preexisting beliefs. One 2015 study of over ten million Facebook users "observed substantial polarization among hard [news] content shared by users, with the most frequently shared links clearly aligned with largely liberal or conservative populations."[149] After the algorithm ranked the stories,[150] Facebook users were slightly less likely to see politically different viewpoints.[151] Individual choice, however, further substantially limited

147. We have discussed the fascinating link between market power and intellectual and regulatory capture at length in *Virtual Competition*. *See* EZRACHI & STUCKE, *supra* note 2, at 244–47.

148. One 2015 study found that sixty–one percent of Millennials (those born between 1981 and 1996) in the United States were "getting political news on Facebook in a given week." Amy Mitchell, Jeffrey Gottfried & Katerina Eva Matsa, *Millennials and Political News: Social Media—The Local TV for the Next Generation?*, PEW RES. CTR. (June 1, 2015), http://www.journalism.org/2015/06/01/millennials-political-news/. This was a much larger percentage than any other news source. *Id.* A 2016 study found that Facebook "sends by far the most mobile readers to news sites of any social media sites"—82 percent of the social traffic to longer news stories and 84 percent of the social traffic to shorter news articles. Katerina Eva Matsa, *Facebook, Twitter Play Different Roles in Connecting Mobile Readers to News*, PEW RES. CTR. (May 9, 2016), http://www.pewresearch.org/fact-tank/2016/05/09/facebook-twitter-mobile-news/. Overall "8% of voters named Facebook as their main source for [2016] election news, outpaced only by Fox News (19% of voters) and CNN (13%)." Jeffrey Gottfried, Michael Barthel & Amy Mitchell, *Trump, Clinton Voters Divided in Their Main Source for Election News*, PEW RES. CTR. (Jan. 18, 2017), http://www.journalism.org/2017/01/18/trump-clinton-voters-divided-in-their-main-source-for-election-news/.

149. Eytan Bakshy et al., *Exposure to Ideologically Diverse News and Opinion on Facebook*, 348 SCIENCE 1130, 1130 (2015).

150. The order in "which users see stories in the News Feed depends on many factors, including how often the viewer visits Facebook, how much they interact with certain friends, and how often users have clicked on links to certain websites in News Feed in the past." *Id.* at 1131.

151. *Id.*

users' exposure to ideologically cross–cutting content.[152] One article asked whether the propagation of fake news before the 2016 U.S. election was an antitrust problem.[153] The fake news problem arose after Facebook implemented product changes that deterred its users from clicking on external news links, and to rely instead on its Instant Articles.[154] Granted, Facebook did not author the fake news stories; but it can manipulate what its two billion users can easily see (and not see). One concern with a dominant digital assistant is that it will not provide an ideologically diverse news stream.[155] Instead a dominant digital assistant will filter the information users receive based on their preexisting preferences, thereby further reducing the viewpoints its users receive and leading to "echo chambers" and "filter bubbles."[156]

Moreover, select groups can manipulate the dominant digital assistant's algorithm to amplify their message. As *The Guardian* reported, Google's autosuggest may be used to propagate biased views against minorities.[157] Partisan groups may also use a more traditional avenue by simply paying the digital assistant for preferential listing.[158] In a world where many users view their search results as unbiased, camouflaged manipulation, as the

152. *Id.*

153. Sally Hubbard, *Why Fake News is an Antitrust Problem*, FORBES (Jan. 10, 2017, 12:00 AM), https://www.forbes.com/sites/washingtonbytes/2017/01/10/why-fake-news-is-an-antitrust-problem/.

154. *Id.*

155. Due to pervasive psychological confirmation biases, users are unlikely to want to hear both the conservative and liberal slant for every news story. *See* Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 155, 210 (2013) ("Particularly when the topic is an emotionally-charged or threatening issue, confirmation bias is a common occurrence.").

156. OECD BACKGROUND NOTE, *supra* note 143, at 43; *see also* ORG. FOR ECON. COOPERATION & DEV., ALGORITHMS AND COLLUSION - NOTE FROM THE EUROPEAN COMMISSION 2 (2017) (noting that when it comes to recommending newspaper articles, personalization can limit the range of views that consumers are exposed to, which is the so-called "filter bubble" or "echo chamber" phenomenon).

157. Carole Cadwalladr, *Google, Democracy and the Truth About Internet Search*, GUARDIAN (Dec. 4, 2016, 5:00 AM), https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook; *see also* Stephanie Bornstein, *Reckless Discrimination*, 105 CALIF. L. REV. 1055, 1102 (2017) ("There is also a serious risk that biasing features could be programmed inadvertently into an algorithm . . . ."); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 671 (2016) (describing discrimination as "unintentional emergent property" from various algorithms).

158. Carole Cadwalladr, *How to Bump Holocaust Deniers Off Google's Top Spot? Pay Google*, GUARDIAN (Dec. 17, 2016, 5:32 PM), https://www.theguardian.com/technology/2016/dec/17/holocaust-deniers-google-search-top-spot.

Russia's influence on the 2016 U.S. presidential elections reflects, becomes a powerful and dangerous tool.[159]

A second risk is censorship, whereby the dominant digital assistant is "programmed to control or block the content that certain users are able to access."[160] The digital assistant can enforce governmental censorship of information with particular religious, political, and social views. For example, in 2017 Apple removed several popular apps that enabled users to evade government censorship from the Chinese version of its app store.[161] Or the super–platform can self–censor as to what is appropriate content. Facebook is grappling with this issue. In 2017, it asked users for input on several questions, including:

> - How aggressively should social media companies monitor and remove controversial posts and images from their platforms?
> - Who gets to decide what's controversial, especially in a global community with a multitude of cultural norms?
> - Who gets to define what's false news — and what's simply controversial political speech? [162]

Ultimately the answers to these questions will come not from users, but the powerful super–platform. It will ultimately decide what news its digital assistant will provide and to whom. One early example occurred when Google's digital assistant censored a Burger King video. According to the *New York Times*, the video stated:

> "You're watching a 15-second Burger King ad, which is unfortunately not enough time to explain all the fresh ingredients in the Whopper sandwich," the actor in the commercial said. "But I got an idea. O.K. Google, what is the Whopper burger?" Prompted by the phrase "O.K. Google," the Google Home device

159. Mike Isaac & Daisuke Wakabayashi, *Russian Influence Reached 126 Million Through Facebook Alone*, N.Y. TIMES (Oct. 30, 2017), https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html; Marguerite Reardon et al., *Congress Grills Facebook, Twitter, Google Over Russian Influence*, CNET (Nov. 1, 2017, 1:56 PM), www.cnet.com/news/congress-grills-facebook-twitter-google-over-russian-influence/.

160. OECD BACKGROUND NOTE, *supra* note 143, at 43.

161. Paul Mozur, *Apple Removes Apps from China Store That Help Internet Users Evade Censorship*, N.Y. TIMES (July 30, 2017), https://www.nytimes.com/2017/07/30/technology/china-apple-censorhip.html.

162. Elliot Schrage, *Introducing Hard Questions*, FACEBOOK (June 15, 2017), https://newsroom.fb.com/news/2017/06/hard-questions/.

> beside the TV in the video lit up, searched the phrase on Wikipedia and stated the ingredients. But within hours of the ad's release — and humorous edits to the Whopper Wikipedia page by mischievous users — tests from The Verge and BuzzFeed showed that the commercial had stopped activating the device. Burger King, which did not work with Google on the ad, said Google appeared to make changes by Wednesday afternoon that stopped the commercial from waking the devices, in what amounted to an unusual form of corporate warfare in the living room. Google, which previously said it had not been consulted on the campaign, did not respond to requests for comment.[163]

Censoring a fast–food restaurant's annoying advertisement may not cause much alarm. In fact, many may welcome it. But Google can also censor its maps, YouTube videos, Google News, AdWords, and search engine results.[164] Thus we can see why conservatives and socialists are raising concerns about Google censoring their viewpoints.[165] Conservatives were also concerned over allegations in 2016 that the social network Facebook manipulated for political purposes the rankings of news stories for its users, suppressing conservative viewpoints.[166] (Facebook denied doing this.)[167]

A third risk is manipulation, whereby the dominant digital assistant's algorithms select information according to particular business or political interests (of the super–platform), instead of its relevance or quality.[168] The

163. Sapna Maheshwari, *Burger King 'O.K. Google' Ad Doesn't Seem O.K. With Google*, N.Y. TIMES (Ap. 12, 2017), https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html.

164. Robert Epstein, *The New Censorship*, U.S NEWS & WORLD REPORT (June 22, 2016, 9:00 AM), https://www.usnews.com/opinion/articles/2016-06-22/google-is-the-worlds-biggest-censor-and-its-power-must-be-regulated.

165. Leo Goldstein, *Google's Search Bias Against Conservative News Sites Has Been Quantified*, WUWT (Sept. 8, 2017), https://wattsupwiththat.com/2017/09/08/a-method-of-google-search-bias-quantification-and-its-application-in-climate-debate-and-general-political-discourse/ ("Google Search is biased in favor of left/liberal websites against conservative websites, and is extremely biased in favor of climate alarmism against climate realism."); *Tucker Warns About 'Ominous' Google Censorship of Political Content*, FOX NEWS INSIDER (Sept. 7, 2017, 9:31 PM), http://insider.foxnews.com/2017/09/07/tucker-ominous-google-censorship-certain-political-content; Peter Hasson, *Anti-Corporate Voices on Both Right and Left Claim Google Censorship*, DAILY CALLER (Aug. 31, 2017, 7:53 PM), http://dailycaller.com/2017/08/31/anti-corporate-voices-on-both-right-and-left-claim-google-censorship/.

166. Deepa Seetharaman, *Facebook Rebuts Criticisms About a Bias Against Conservatives*, WALL ST. J. (May 10, 2016, 8:41 AM), www.wsj.com/articles/facebook-refutes-criticisms-about-a-bias-against-conservatives-1462890206.

167. *Id.*

168. OECD BACKGROUND NOTE, *supra* note 143, at 43.

composition and order of the news feed can affect users' inclinations. With sixty–one percent of Millennials relying on the social network to receive their news, the power of the network becomes clear. Users rely on the super–platforms, in part, because they believe the algorithms objectively identify the most relevant results.[169] But Google's conduct with Froogle demonstrates, a powerful platform can intentionally degrade the quality of its search results to promote its own corporate interests. Robert Epstein illustrated how Google, in manipulating the rankings of its search results, could shift the voting preferences of undecided voters by "20 percent or more—up to 80 percent in some demographic groups—with virtually no one knowing they are being manipulated."[170] Other dominant super–platforms like Facebook can also manipulate elections.[171] Jonathan Zittrain has warned of the super–platform's potential ability to predict political views, identify party affiliation, and engage in targeted campaigning to mobilize distinct groups of voters to take action.[172] Indeed, Russian operatives established competing Facebook groups, the chair of the Senate Intelligence Committee noted, to "fuel divisions among Americans."[173]

Super–platforms have already used their market dominance to promote certain corporate agendas. Google, for example, used its homepage to protest against the Stop Online Piracy Act, asking users to petition Congress.[174] Consumer Watchdog, in comparing the search results of Bing, DuckDuckGo, and Google, accused Google of "manipulating its search engine results to favor opposition" to Section 230 of the Communications Decency Act.[175] Google was leading the "[t]ech industry efforts to block

169. Claire Cain Miller, *When Algorithms Discriminate*, N.Y. TIMES (July 9, 2015), https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html.

170. Robert Epstein, *How Google Could Rig The 2016 Election*, POLITICO (Aug. 19, 2015), http://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548.

171. Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.

172. *Id.*

173. Mary Louise Kelley, Ryan Lucas & Richard Burr, *How Russia Used Facebook to Organize 2 Sets of Protesters*, NPR (Nov. 1, 2017, 4:53 PM), https://www.npr.org/2017/11/01/561427876/how-russia-used-facebook-to-organize-two-sets-of-protesters.

174. Jared Newman, *SOPA and PIPA: Just the Facts*, PCWORLD (Jan. 17, 2012, 6:00 PM), https://www.pcworld.com/article/248298/sopa_and_pipa_just_the_facts.html.

175. John M. Simpson, *Google Appears to Be Manipulating Its Search Engine Results to Defend Internet Law that Enables Sex Trafficking, Consumer Watchdog Finds*, CONSUMER WATCHDOG (Sept. 11, 2017), http://www.consumerwatchdog.org/newsrelease

any amendment to Section 230, which protects websites from liability for material posted by third parties on their sites."[176] As Consumer Watchdog found, "[t]hree of the top four links returned under the news tab for the search term 'Section 230' were to articles from the Electronic Frontier Foundation, a staunch opponent of amending the Internet law."[177] In contrast, Bing and DuckDuckGo "gave links to articles presenting all sides of the issue."[178]

As the European Commissioner concluded:

> The way that algorithms are used to make decisions automatically could even undermine our democracy. These days, social media is a vital source of news. One recent study found that nearly two thirds of US adults get their news this way. So the scope for social media algorithms to create an alternative reality, by showing people one story after another that just isn't true, is a concern for us all."[179]

If users increasingly rely on one digital assistant, it will increasingly learn about many citizens' social and political views, behavior, and susceptibility to biases. Facebook, for example, "collects data on roughly 1.6 billion people, including 'likes' and social connections, which it uses to look for behavioral patterns such as voting habits, relationship status and how interactions with certain types of content might make people feel."[180] But Facebook does not simply passively collect data about its users; it also has the power to affect behavior. One study, which later proved quite controversial, sought to examine "emotional contagion," whereby people transfer positive and negative moods and emotions to others.[181] This was the "first experimental evidence for massive-scale emotional contagion via

/google-appears-be-manipulating-its-search-engine-results-defend-internet-law-enables-s-0.

176. *Id.*

177. *Id.*

178. *Id.*

179. Margrethe Vestager, Comm'r, European Comm'n for Competition, Algorithms and Competition, Address at Bundeskartellamt 18th Conference on Competition (Mar. 16, 2017), https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017_en.

180. Daniela Hernandez & Deepa Seetharaman, *Facebook Offers Details on How It Handles Research*, WALL ST. J. (June 14, 2016), http://www.wsj.com/articles/facebook-offers-details-how-it-handles-research-1465930152.

181. Adam D. I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L ACAD. SCI. 8788 (2014).

social networks."[182] People, when posting of Facebook, frequently express positive or negative emotions.[183] Their friends later see these posts via Facebook's "News Feed" product. Facebook uses a ranking algorithm that continually tests which content is shown or omitted in the News Feed.[184] The aim is to show particular Facebook users "the content they will find most relevant and engaging."[185] Facebook, as part of the study, intentionally manipulated its News Feed algorithm.[186] Some users received less positive content.[187] Other received less negative emotional content.[188]

Did that manipulation impact what the 689,003 test subjects posted?[189] It did. When Facebook surreptitiously reduced friends' positive content in the News Feed for one week, the users were less positive: "a larger percentage of words in the users' status updates were negative and a smaller percentage were positive."[190] When Facebook surreptitiously reduced their friends' negative content in the News Feed, the Facebook users were less negative themselves. People who were exposed to fewer emotional posts (either positive or negative) in their News Feed "were less expressive overall on the following days."[191] Thus by manipulating the News Feed, Facebook could influence users' moods.

Interestingly, Facebook could manipulate users' emotions without prohibiting users from accessing content. The users' search costs were low, because their friends' content:

> was always available by viewing a friend's content directly by going to that friend's wall" or "timeline," rather than via the News Feed. Further, the omitted content may have appeared on prior or subsequent views of the News Feed. Finally, the experiment did not affect any direct messages sent from one user to another.[192]

If Facebook can affect a user's mood and engagement by simply promoting some content over another in the user's News Feed, just imagine the power

182. *Id.* at 8789.
183. *Id.* at 8788.
184. *Id.*
185. *Id.*
186. *Id.*
187. *Id.* at 8788–89.
188. *Id.*
189. *Id.*
190. *Id.* at 8789.
191. *Id.* at 8790.
192. *Id.* at 8789.

of a dominant digital assistant to affect citizens' moods, behavior, and views.

Ultimately, in a world where digital assistants play a key role as a gateway to news, they will have the power to affect its composition. Without noticing, citizens could outsource the task of shaping their world view to a dominant corporation. Normally, with power comes great responsibility.[193] That is indeed the case in EU competition law when a firm dominates markets for goods and services.[194] This concern of the super–platform's shirking of this responsibility arose with fake news. As worldwide web inventor Tim Berners-Lee noted:

> Today, most people find news and information on the web through just a handful of social media sites and search engines. These sites make more money when we click on the links they show us. And, they choose what to show us based on algorithms which learn from our personal data that they are constantly harvesting. The net result is that these sites show us content they think we'll click on – meaning that misinformation, or 'fake news', which is surprising, shocking, or designed to appeal to our biases can spread like wildfire. And through the use of data science and armies of bots, those with bad intentions can game the system to spread misinformation for financial or political gain.[195]

Thus, when a few gatekeepers dominate the digital assistant market, economic power can translate into political power—be it through payment by third parties or as a result of the platform itself opting to advance one agenda over another. The marketplace of ideas, just like online markets for goods and services, may be manipulated.

---

193. Meng Ding, Perfect 10 v. Amazon.com*: A Step Toward Copyright's Tort Law Roots*, 23 BERKELEY TECH. L.J. 373, 373 (2008) (quoting SPIDER-MAN (Columbia Pictures 2002)).

194. Case C-413/14 P, Intel Corp. v. Commission, ¶ 135 (Sept. 6, 2017), http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5d76741cb58524179974ae33bfb72e370.e34KaxiLc3eQc40LaxqMbN4PaN8Oe0?text=&docid=194082&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=195067 ("[A] dominant undertaking has a special responsibility not to allow its behaviour to impair genuine, undistorted competition on the internal market").

195. Tim Berners-Lee, *Three Challenges for the Web, According to Its Inventor*, WORLD WIDE WEB FOUND. (Mar. 12, 2017), http://webfoundation.org/2017/03/web-turns-28-letter/.

C. PRIVACY CONCERNS

Smartphones currently collect and store an immense amount of data (including information that users may not ever use, such as their movements or search history).[196] As Google, Apple, Facebook and other leading tech firms told the Supreme Court in 2017:

> People search online for all manner of information, including medical advice, and rely on the Internet for their jobs, schooling, and interpersonal communications. They reveal their habits, views, and preferences by interacting with apps used to navigate almost every facet of their lives. They store photos and emails in the cloud, rely on data-collecting devices such as fitness trackers to manage their health, and use smart appliances to provide home security and efficiency. For many of these activities, there is no analog-era analogy; in the past, for instance, a user did not have to tell a company when and how he wanted to adjust his thermostat, thereby risking losing all privacy protection in that information.[197]

Digital assistants (and the smart technologies connected with them) aim to collect even more personal data. A 2017 criminal case offers a glimpse at the potential privacy implications created by digital assistants. The Bentonville Police Department in Arkansas was investigating a death at the defendant's residence.[198] The defendant was charged with first–degree murder.[199] While searching the defendant's residence, the police seized an Echo device.[200] The police next served Amazon with a warrant seeking any audio recordings and transcripts that were created as a result of interactions with defendant's Amazon Echo.[201] Citing "important First Amendment and privacy implications at stake," Amazon sought to quash the search warrant

196. Brief for Technology Companies as Amici Curiae in Support of Neither Party at 18, Carpenter v. United States, No. 16-402, 2017 WL 3530959 (U.S. Aug. 14, 2017) ([hereinafter *Carpenter Amicus Brief*]. Nest Labs, which manufactures smart thermostats, and its parent Google were among the amici. *Id.*

197. *Id.* at 27.

198. Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant at 6, State v. Bates, No. CR-2016-370-2 (Cir. Ct. Ark., Feb. 17, 2017) [hereinafter *Amazon Memorandum*].

199. *Id.*

200. *Id.*

201. *Id.*

"unless the Court finds that the State has met its heightened burden for compelled production of such materials."[202]

As Amazon told the court, the privacy concerns were significant. Its digital assistant "can be commanded to, among other things, play music, stream podcasts, play audio books, request information about various subjects, or request 'real-time information,' including news, weather, and traffic conditions related to the user's or any other location."[203] As one example, "users may ask for information about a sensitive health condition or a controversial political figure."[204] Users can also use their digital assistant to order products from Amazon, including books and other expressive materials. Thus, the digital assistant sweeps in significant amounts of data that can "reveal much more in combination than any isolated record." [205] Those with access to the data can reconstruct "[t]he sum of an individual's private life."[206]

Amazon was concerned with governmental invasions of its users' privacy and First Amendment interests. As Amazon cautioned, "the knowledge that government agents are seeking records concerning customer purchases of expressive material from Amazon 'would frost keyboards across America.'"[207] Indeed, "'rumors of an Orwellian federal criminal investigation into the reading habits of Amazon's customers could frighten countless potential customers' into cancelling their online purchases through Amazon, 'now and perhaps forever,' resulting in a chilling effect on the public's willingness to purchase expressive materials."[208]

Eventually, after the defendant consented, Amazon disclosed the information to the State.[209] But government surveillance remains a concern. Facebook, Apple, and Google, among others, recently impressed this point

202. *Id.* at 1. Amazon argued that the State must demonstrate: (1) a compelling need for the information sought, including that it is not available from other sources; and (2) a sufficient nexus between the information and the subject of the criminal investigation. *Id.* at 2.

203. *Id.* at 5.

204. *Id.*

205. *Id.* at 9 (quoting Riley v. California, 134 S. Ct. 2473, 2489 (2014)).

206. *Id.* (quoting *Riley*, 134 S. Ct. at 2489).

207. *Id.* at 14 (quoting *In re* Grand Jury Subpoena to Amazon.com Dated August 7, 2006, 246 F.R.D. 570, 573 (W.D. Wis. 2007) [hereinafter *Grand Jury Subpoena*]).

208. *Id.* (quoting *Grand Jury Subpoena*, 246 F.R.D. at 573).

209. Andrew Blake, *Amazon Gives Up Alexa Data Sought in Murder Probe*, WASH. TIMES (Mar. 8, 2017), http://www.washingtontimes.com/news/2017/mar/8/amazon-gives-alexa-data-sought-murder-probe/.

to the Supreme Court: "While amici's customers understand that data is collected by service providers as part of providing digital technologies, customers still expect privacy with respect to other parties, including the government."[210] As the amici argued, "[d]igital technologies have become a necessary aspect of life today."[211] Individuals cannot realistically forgo these technologies; nor can users of these digital technologies avoid transmitting sensitive data to the technologies' service providers. Nonetheless, users expect that data to remain private.[212]

But it is questionable whether the accused can challenge under the Fourth Amendment any warrantless search or seizure of data Amazon's digital assistant collects from individuals. This is because the accused—under a line of Supreme Court cases—would have no reasonable expectation of privacy in the data they share with third parties, like Amazon.[213]

Another concern is covert government surveillance. One example, according to WikiLeaks documents disclosed on the subject, is the Central Intelligence Agency's "Weeping Angel" program. The CIA basically

210. *Carpenter Amicus Brief*, *supra* note 196.

211. *Id.* at 13.

212. *Id.* at 17. The amici rely in part on a poll by the Pew Research Center, where "93% of adults say that being in control of who can get information about them is important: 74% feel this is 'very important'; 19% say it is 'somewhat important.' 90% say that controlling what information is collected about them is important—65% think it is 'very important' and 25% say it is 'somewhat important.'" *Id.* at 19 n.3 (quoting Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/). Additionally, "Americans say they do not wish to be observed without their approval; 88% say it is important that they not have someone watch or listen to them with- out their permission (67% feel this is 'very important' and 20% say it is 'somewhat important')." *Id.*

213. United States v. Miller, 425 U.S. 435, 443 (1976) (holding that the government, consistent with the Fourth Amendment, can obtain "information revealed to a third-party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third-party will not be betrayed"); Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals when Third Parties Are Forced to Hand Over Passwords*, 30 BERKELEY TECH. L.J. 1, 14 (2015) (explaining that the third–party doctrine strips users of privacy rights in stored passwords); Mark Daniel Langer, *Rebuilding Bridges: Addressing the Problems of Historic Cell Site Location Information*, 29 BERKELEY TECH. L.J. 955, 965 (2014) (criticizing application of the third–party doctrine to location information gathered from smartphones); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1250 (2009) (criticizing the third–party doctrine generally).

hacked smart televisions, transforming them into covert microphones.[214] "After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server."[215] The CIA could also remotely hack and control popular smartphones, which could be instructed to send the CIA "the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone."[216] Presumably, other governments would have similar incentives and ability to hack digital assistants to monitor and gather evidence. In an unconcentrated digital assistant market, personal data is dispersed across many firms. In contrast, in a monopolized market, personal data is concentrated in one or few firms. This increases the government's incentive to circumvent the firm's privacy protections and tap into the digital assistant's capabilities.[217] Also, the fewer the number of firms controlling the personal data, the risk increases that the government will "capture" the firms, using its many levers.[218]

But another privacy concern, which Amazon did not address in its court filing, is the private collection and use of this data. A 2017 FTC case against the television manufacturer VIZIO suggests the extent to which private

214. Press Release, Wikileaks, Vault 7: CIA Hacking Tools Revealed (Mar. 7, 2017), https://wikileaks.org/ciav7p1/.

215. *Id.*

216. *Id.*

217. *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links To Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

218. Kelton Sears, *Alexa and the Dawn of So-What Surveillance*, SEATTLE WEEKLY (Mar. 29, 2017, 1:30 AM), http://www.seattleweekly.com/news/alexa-and-the-dawn-of-so-what-surveillance/. On the one hand, a dominant firm might have the resources to fight off the government. On the other hand, as personal data is spread out across many firms, there are more firms that the government would have to bribe (or coerce) to access the data. As the number of bribes increase, the lower the likely value of each bribe to each firm possessing the personal data, and the greater the likelihood that the bribe will be less than the value to the digital assistant producer for securing the data. Moreover, a dominant firm is likely to lobby the government on many more fronts. Brian Fung & Hamza Shaban, *To Understand How Dominant Tech Companies Are, See What They Lobby For*, L.A. TIMES (Sept. 1, 2017, 12:55 PM), http://www.latimes.com/business/technology/la-fi-tn-silicon-valley-lobbying-20170901-story.html. This can increase the likelihood of secretly cooperating with the government in accessing the data if doing so yields greater benefits on the other fronts.

collection might have dangerous implications for consumer rights.[219] The FTC alleged that since February 2014, VIZIO televisions continuously tracked what consumers were watching.[220] Over ten million VIZIO televisions transmitted information about what the viewer was watching "on a second-by-second basis."[221] Why the intrusive tracking? VIZIO profited from selling the consumers' television viewing history to third parties.[222] One purpose for the viewing data was to analyze advertising effectiveness. With the VIZIO TV data, third parties could analyze a household's behavior across devices, for example, "(a) whether a consumer has visited a particular website following a television advertisement related to that website, or (b) whether a consumer has viewed a particular television program following exposure to an online advertisement for that program."[223] Another purpose for the viewing data was to better target the household members on their other digital devices.[224]

VIZIO eventually settled.[225] An outstanding legal issue was whether VIZIO's disclosure was "unfair" or "deceptive" under section 5 of the FTC Act. As the FTC alleged, consumers were never directly informed that their new VIZIO televisions were tracking their viewing habits or selling this data to better target them with personal ads.[226] The acting FTC Chair concurred in the enforcement action only because VIZIO deceptively omitted information about its data collection and sharing program.[227] But she did not support the count in the complaint alleging that VIZIO's collection and sharing of the data without consumers' consent was inherently "unfair."[228]

---

219. Complaint for Permanent Injunction and Other Equitable and Monetary Relief, FTC v. VIZIO, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) [hereinafter *FTC Complaint*], https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.

220. *Id.* at 4.

221. *Id.*

222. *Id.* at 5.

223. *Id.*

224. *Id.*

225. Press Release, Fed. Trade Comm'n, VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

226. *See FTC Complaint*, *supra* note 219, at 9.

227. *In re* Vizio, Inc., FTC File No. 1623024 (Feb. 6, 2017) (concurring statement of Acting Chair Maureen K. Ohlhausen), https://www.ftc.gov/public-statements/2017/02/concurring-statement-acting-chairman-maureen-k-ohlhausen-matter-vizio-inc.

228. *Id.*

The VIZIO enforcement action illustrates the privacy implications of a dominant digital assistant. First, it appears that a dominant digital assistant can collect this personal information. Based on the Acting Chair's construction of the FTC Act, a super–platform can use its digital assistant to track consumers, collect their data, develop personal profiles, and target them with behavioral ads. It can even sell that data to third parties. All that seems to be required is that it discloses the collection and use of data to consumers. But suppose Amazon or Google state broadly in its privacy statement that the data it collects across its products and services is used for advertising purposes. Whether or not this disclosure is sufficient to infer consent remains unclear.[229]

A second issue is what constitutes consent and who must consent. The FTC complaint focused on consumers that purchased VIZIO televisions. But a dominant digital assistant will sweep in data from children, other household members, relatives, friends, and others in the house. With facial recognition technology, a dominant digital assistant can track individuals across neighborhoods and cities.[230] It is unclear whether the super–platform has to inform (or obtain consent from) anyone besides the purchaser of the tracking.

A third issue is control over the data. Nothing under the current U.S. law provides adults (or teenagers) with a way to review the personal information that the dominant digital assistant collected about them, nor does current law give them a way to revoke their consent and refuse the further use or collection of personal information, or to delete already–retained personal information.[231]

Ultimately consent has less significance when dealing with a monopoly.[232] Firms can exercise market power multiple ways, such as

229. *Amazon Privacy Notice*, AMAZON (Aug. 29, 2017), https://www.amazon.com/gp/help/customer/display.html?nodeId=468496.

230. *Nowhere to Hide: What Machines Can Tell from Your Face*, ECONOMIST (Sept. 9, 2017), https://www.economist.com/news/leaders/21728617-life-age-facial-recognition-what-machines-can-tell-your-face.

231. The Children's Online Privacy Protection Act of 1998, which affords these protections, applies to data collected on children under thirteen years old. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2017).

232. US Airways, Inc. v. Sabre Holdings Corp., No. 11 CIV. 2725 (LGS), 2017 WL 1064709, at *13 (S.D.N.Y. Mar. 21, 2017) (evidence of market power includes forcing customers "to do things they would not do in a competitive market, such as signing contracts with terms they would not otherwise accept").

raising price or reducing quality.[233] One facet of competition for "free" goods is privacy protection.[234] Just as a monopoly retailer can increase price above competitive levels, so too a dominant digital assistant can depress privacy protections below competition levels.[235] As the European Commission found when reviewing the Microsoft/LinkedIn merger, consumer choice and privacy protection would be substantially reduced.[236] A dominant digital assistant could collect more personal data and provide less privacy protection than it otherwise could in a competitive market.[237] Users would have no real choice.[238] Instead, they would have to rely on the monopolist's beneficence for any privacy protections. This is especially troubling when the digital assistant is connected not only to a user's TV set, but to computers, smart appliances, security cameras, smartphones, and smart cars, as well as the super–platform's other services (such as search engines, email, maps, and the like).

Thus, unlike monopolies of the past, a dominant digital assistant will know far more intimate details about consumers.[239] Even something as innocuous as a smart thermometer can detect and transmit "not just a

233. U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, HORIZONTAL MERGER GUIDELINES 2 (2010), www.justice.gov/atr/horizontal-merger-guidelines-08192010 ("A merger enhances market power if it is likely to encourage one or more firms to raise price, reduce output, diminish innovation, or otherwise harm customers as a result of diminished competitive constraints or incentives.").

234. STUCKE & GRUNES, *supra* note 40, at ch. 17.

235. *Id.*; Press Release, European Comm'n, Mergers: Commission Approves Acquisition of LinkedIn by Microsoft, Subject to Conditions (Dec. 6, 2016), http://europa.eu/rapid/press-release_IP-16-4284_en.htm ("[T]he Commission concluded that data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction.").

236. *See, e.g.*, *Microsoft/LinkedIn Decision*, *supra* note 22, ¶ 350 ("[T]o the extent that these foreclosure effects would lead to the marginalisation of an existing competitor which offers a greater degree of privacy protection to users than LinkedIn (or make the entry of any such competitor more difficult), the Transaction would also restrict consumer choice in relation to this important parameter of competition when choosing" a professional social network).

237. Eleonora Ocello & Cristina Sjödin, Microsoft/LinkedIn*: Big Data and Conglomerate Effects in Tech Markets*, EUR. COMMISSION: COMPETITION MERGER BRIEF 5 (May 2017), http://ec.europa.eu/competition/publications/cmb/2017/kdal17001enn.pdf (discussing how the foreclosure of competing networks post-merger could adversely impact the choice of consumers as to the level of data protection offered, as some competitors offered a greater degree of privacy protection to users than LinkedIn).

238. *Id.*

239. *Carpenter Amicus Brief*, *supra* note 196, at 25 (noting how "digital devices and services produce and record data that, alone or in the aggregate, has the potential to reveal highly sensitive information about all aspects of our private lives").

home's temperature, but information about the homeowner's habits—whether and when the occupants are home, and where they are in the home."[240]

Nor does simply shutting off the digital assistant offer a viable alternative in a modern world that is so heavily dependent on integrated technology. A total ban on internet use, the Seventh Circuit found back in 2003, would sweep more broadly and impose a greater deprivation on defendant's liberty than was necessary: "such a ban renders modern life—in which, for example, the government strongly encourages taxpayers to file their returns electronically, where more and more commerce is conducted on-line, and where vast amounts of government information are communicated via website—exceptionally difficult."[241] Smartphones, as the Supreme Court recognized, "are now such a pervasive and insistent part of daily life."[242] The Court cited one 2013 poll where "nearly three-quarters of smartphone users report being within five feet of their phones most of the time, with 12 percent admitting that they even use their phones in the shower."[243] More than twice as many respondents in another poll "were willing to give up sex instead of their smart phone or caffeine."[244] With the rise of smart appliances, it will be even harder to turn off a digital assistant and smartphone.[245]

But if any super–platform abused its position of trust, some might respond, one can turn to more privacy–focused alternatives. Yes Google, Apple, Facebook, and Amazon may strive to be the dominant digital assistant. But other companies may launch competing assistants. Thus, if a super– platform failed to respect users' privacy, one issue is whether users would opt for another digital assistant. As this Part explored, however, market competition may not effectively cure these privacy concerns because users may be unaware of some of the tactics the super–platform deploys to increase its profitability while undermining its users' welfare. Another problem, as the next Part explores, is that the ability to switch digital assistants may be more limited than one might anticipate.

240. *Id.*
241. United States v. Holm, 326 F.3d 872, 877 (7th Cir. 2003).
242. Riley v. California, 134 S. Ct. 2473, 2484 (2014).
243. *Id.* at 2490.
244. *Poll: Americans Choose Smartphones Over Sex*, SACHS MEDIA GRP. (Apr. 12, 2017), https://sachsmedia.com/news/poll-americans-choose-smartphones-over-sex/.
245. *Carpenter Amicus Brief*, *supra* note 196, at 16 (noting how forgoing the use of networked devices would render modern life exceptionally difficult).

IV. WHY THE LEADING DIGITAL ASSISTANT WILL LIKELY BE FROM GOOGLE, APPLE, FACEBOOK, OR AMAZON

With the possibility that a digital assistant can act against its users' interest, one would expect and hope for a "virtuous assistant"—a class of independent assistants, developed by independent firms that prioritized consumer interests. These virtuous assistants could warn users when behavioral discrimination is at play, when outside options are ignored, when price alignment seems out of order, or when personal data is collected. They may even deploy countermeasures to maximize user welfare in the face of such strategies. They could monitor news feed and alert users if they are targeted with particular stories (or missing stories from traditional journalism outlets). They can promote users' interest—aware of their preferences and safeguarding their autonomy.

Predicting the leading technology five years from now is tricky. But several factors favor one of the four super–platforms (Google, Apple, Amazon, and Facebook) capturing the digital assistant market, and disfavoring an independent virtuous assistant. To work well (and gain popularity), the digital assistant will likely have to operate from an existing platform—such as a mobile platform—and in order to tap into the vast wealth of preexisting data offered by such platforms. This is true for several reasons: first, the scale and scope of data needed favor emergence from a platform; second, the data–driven network effects are best effectuated by a platform, and third, platforms can facilitate the integration of the digital assistant with other apps and services, such as texts, mapping, photographs, and more.

Personal data is the first key element. To provide relevant services and recommendations, the digital assistant must first learn the user's habits and preferences. To learn their preferences and predict the users' desires, digital assistants will require a significant volume and variety of personal data. Absent these features, an "isolated" helper would be of little use and value—indeed, it would not be a *personal* digital assistant. Based on the user's personal data—including chat history, geolocation, previous purchasers, and browsing habits—the digital assistant can provide and anticipate personalized recommendations.

Some argue that the value is not from the data or the data–driven network effects, but the algorithms that process the data. But if this were true, noted Lukas Biewald, co–founder and CEO of CrowdFlower, the big tech players IBM, Facebook, Google, and Microsoft would not open source some of their algorithms "without worrying too much about giving away

any secrets."[246] As Biewald noted, "it's because the actual secret sauce isn't the algorithm, it's the data. Just think about Google. They can release TensorFlow without a worry that someone else will come along and create a better search engine because there are over a trillion searches on Google each year."[247] Another example is Facebook's M, where the underlying code and algorithms are largely open source.[248] The key assets are not the algorithms—otherwise, why would Facebook share them? Instead, the key is the combination of the scale and scope of data, and the algorithm's ability to learn by trial–and–error. As the *Wall Street Journal* reported, "Facebook Messenger already has more than 700 million users," which yields it the following advantage: "with access to so many users, Facebook has a plausible way to get the gigantic quantity of conversational data required to make a chat-based assistant sufficiently automated."[249] With more users making more requests, M can quickly process more tasks easily.[250] By learning through servicing users, digital assistants can take a proactive role—anticipating the user's needs and wants—rather than merely following instructions. This requires the platform to have enough users, data, and opportunities to experiment to train the algorithms.[251] The super–platforms already possess far more personal data than any startup could readily and affordably obtain.[252] New entrants will be at a significant disadvantage. Any independent virtuous assistant will likely lack the scale

246. Daniel Gutierrez, *Human-in-the-Loop is the Future of Machine Learning*, INSIDEBIGDATA (Jan. 11, 2016), http://insidebigdata.com/2016/01/11/human-in-the-loop-is-the-future-of-machine-learning/.

247. *Id.*

248. Mims, *supra* note 17.

249. *Id.*

250. *Id.*

251. STUCKE & GRUNES, *supra* note 40, at 181–82.

252. *Japan's Antimonopoly Law At Turning Point*, STANDARD EXAM'R (Sept. 18, 2017, 9:56 AM), http://www.standard.net/Business/2017/09/18/Japan-s-antimonopoly-law-at-turning-point; *Fuel of the Future: Data Is Giving Rise to a New Economy*, ECONOMIST (May 6, 2017), https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy; Franklin Foer, *How Silicon Valley Is Erasing Your Individuality*, WASH. POST (Sept. 8, 2017), https://www.washingtonpost.com/outlook/how-silicon-valley-is-erasing-your-individuality/2017/09/08/a100010a-937c-11e7-aace-04b862b2b3f3_story.html; Rana Foroohar, *Big Tech's Power Remains Unchallenged*, FIN. TIMES (Sept. 19, 2017), https://www.ft.com/video/19982ee4-0468-4efe-8e06-86057bb728e7.

and scope of data (to train their digital assistant), as well as the products necessary to attract new users and convince existing users to switch.[253]

Network effects are the second key element. As we saw, traditional network effects help the leading platform attract more developers and smart–technology manufacturers. Plus, the "learning–by–doing" and "scope" network effects improve the quality of super–platform's algorithm in predicting users' needs and tastes. Only a few companies in mid–2017 have the requisite volume and variety of personal data and opportunities to experiment for their digital assistants to be competitive: Amazon, Facebook, Google, and Apple.

The third key element is the scope of services the personal assistant can offer, and the extent to which the digital assistant is integrated in these other services. The European Commission's recent decision in the *Microsoft/LinkedIn* merger is instructive on how integration, at times, can foreclose competition.[254] Before the Commission approved the transaction, it noted the possible adverse effects which could result from the integration of LinkedIn's features into the existing Microsoft platform.[255] Such integration would make the LinkedIn features "particularly prominent" to Microsoft Outlook users and "likely enhance LinkedIn's visibility to a very large number of users" more so than when LinkedIn was a stand–alone professional social network.[256] This would increase the size of the professional social network (and use of the network effects to Microsoft's advantage).[257] Second, Microsoft could leverage its platform (such as Outlook users' address books) to suggest new LinkedIn connections and thereby further significantly expand the size of its professional social network.[258] While LinkedIn would increase in size (and power), Microsoft could hinder competing professional social networks by denying access to

253. Sofia Grafanaki, *Autonomy Challenges in the Age of Big Data*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 803, 841 (2017) (noting how the winner in the race among digital assistants "will most likely depend on which company can create the most seamless experience across devices and platforms. In other words, the key is the aggregation of personal information.").

254. *See, e.g.*, *Microsoft/LinkedIn Decision*, *supra* note 22, ¶ 330 (noting how integrating LinkedIn features into Microsoft Office, while denying competing professional social network service providers access to Microsoft APIs may foreclose competing providers).

255. Press Release, *supra* note 235.

256. *See, e.g.*, *Microsoft/LinkedIn Decision*, *supra* note 22, ¶ 328.

257. *Id.* ¶ 324.

258. *Id.* ¶ 328.

its Outlook API (and potentially other Microsoft APIs).[259] If Microsoft did so, "such providers would likely have no counterstrategy at their disposal to sufficiently counter the merged entity's actions."[260] As a result, such integration would likely increase the LinkedIn platform's size and usage in a way that rivals could not match.[261] Due to the network effects, LinkedIn would continue growing toward dominance, and competing professional social network providers would be unable to compete effectively.[262]

The Commission's concern in *Microsoft/LinkedIn* was the emergence of a durable monopoly and its concomitant effects.[263] Likewise, the super–platform can nudge users to its digital assistant by seamlessly integrating its digital assistant with its wide offering. Google, for example, announced in 2017 that it was incorporating artificial intelligence into its Gmail service—which is used by over a billion people—"for features such as suggesting responses to messages."[264] Google, as the chief digital assistant, can analyze our emails, texts, or photos, and suggest replies.[265] Google argues that given:

> its 17 years of work cataloguing the internet and physical world, its assistant is smarter and better able to work with its email, messaging, mapping and photo apps. And since Google makes software for smartphones, smartwatches and old-fashioned computers, Google says people will be able to have one conversation with multiple machines.[266]

A standalone virtuous assistant would be at a disadvantage. As Google told developers in 2017, its Android mobile operating system is used on over two billion active devices worldwide; its Google Play online store, Google Maps, Gmail, Chrome operating system and search app all have over one billion monthly users.[267] Developing a platform of similar scale

259. *Id.* ¶ 329.
260. *See, e.g.*, *id.*
261. *Id.* ¶ 330.
262. *Id.* ¶ 343.
263. *Id.* ¶ 348.
264. *Google Assistant Coming to iPhones; Will Take on Siri*, WION (May 18, 2017, 1:11 PM), https://www.wionews.com/science-tech/google-assistant-coming-to-iphones-will-take-on-siri-15719.
265. Yadron, *supra* note 10.
266. *Id.*
267. Reinhardt Krause, *Google Trumpets Platform User Base vs. Apple, Facebook, Amazon*, INV. BUS. DAILY (May 18, 2017), http://www.investors.com/news/technology/google-trumpets-platform-user-base-vs-apple-facebook-amazon/.

and scope from scratch would likely be too costly and time consuming for a competitor. For example, Microsoft spent over "$4.5 billion into developing its algorithms and building the physical capacity necessary to operate" its search engine Bing.[268] Thus, a standalone virtuous assistant would likely need to access and function well with the super–platform's services.

Super–platforms have already taken steps in order to consolidate market power. Amazon in 2017, for example, partnered with Microsoft so that its digital assistant will get better functionality via Cortana by accessing Microsoft users' work calendars and emails.[269] Before then "Amazon, Microsoft, Apple, and Google ha[d] all built rival digital assistants that have been seen as walled gardens blocked off from each other, and this partnership signals a move to make them work better together."[270]

While Amazon and Microsoft might agree to partner with each other, and while Apple might be willing to have Google's digital assistant operate on its iPhone,[271] a dominant super–platform may not allow a nascent virtuous assistant to access its platform and users.[272] It could deny access to the Google Play online store and Apple's App Store.[273] It could restrict access to its user's calendar, email, or texting app. It could give preferential

268. FED. TRADE COMM'N, MEMORANDUM RE: GOOGLE INC FILE NO. 111-0163 at 76 (2012), http://graphics.wsj.com/google-ftc-report (hosting the inadvertently–leaked report).

269. Tom Warren, *Microsoft and Amazon Partner to Integrate Alexa and Cortana Digital Assistants*, VERGE (Aug. 30, 2017, 4:11 AM), https://www.theverge.com/2017/8/30/16224876/microsoft-amazon-cortana-alexa-partnership.

270. *Id.*

271. Reinhardt Krause, *Siri, What's Coming to Apple iPhones? Google's Digital Assistant*, INV. BUS. DAILY (May 16, 2017), http://www.investors.com/news/technology/siri-whats-coming-to-apple-iphones-googles-ai-digital-assistant/.

272. *See, e.g.*, Grafanaki, *supra* note 253, at 841:

> Because users pay companies like Google with their attention and their data, which the companies then convert to advertising revenue, Google's incentive is to keep users "locked-in" to its services in order to keep collecting information, even if competitors may offer better products. Such efforts are also present in Google's new product development in an attempt to harness the momentum that is moving away from desktop search and direct it to other products that the company can use as platforms for its advertising business. This would seem like a simple rule of business, but for the fact that Google is also the way that users find potentially competing products, raising concerns about some of its practices.

273. *See* EZRACHI & STUCKE, *supra* note 2, at 184–86 (discussing Disconnect being kick out of Google Play Store).

treatment to its own digital assistant, by pre–loading it on its smartphone, having it on the smartphone's opening screen, or integrating it into its other popular products, including its search engine and the operating system.[274] It may exclude the virtuous assistant from its online wallet, such as Apple Pay or Google Wallet.[275] It could degrade the virtuous assistant's functionality by having it run slower than the operating system's digital assistant.[276] Users would likely blame the virtuous assistant for its tardiness. Or the super–platforms may simply block the virtuous assistant by arguing that doing so protects its users. For example, the super–platform may argue that privacy considerations restrict interoperability with the virtuous assistant.[277]

Consequently, at least three key elements—data, network effects, and scope of platform's services—increase the likely switching costs and undermine a potential virtuous assistant's success. Although these elements favor the super–platform, a popular virtuous assistant remains possible. Despite the possibility for such a virtuous assistant, we are rather pessimistic. Perhaps the easiest way to explain our pessimism is to ask the following: Which search engine did you use today (or this past week)? Did you opt for one which does not harvest information and retains your anonymity (such as DuckDuckGo) or for one which tracks your behavior to better target you with personalized ads? Did you limit the ability of your phone apps to access personal and geolocation information? Do you often change the default option? When downloading an app or update, do you read the terms and conditions? Even if you did, did you still accept the terms—despite not certainly knowing who will access your data and what they will do with it?

In sum, a virtuous assistant is possible. Its presence might possibly limit the ability of the dominant digital assistant to abuse its power. But in reality, the majority of users may lack the incentive to switch. They may find it difficult to quantify cost and harm, and when faced with complex decision making, they may opt for the default. To illustrate—despite the European Commission's record fine against Google and Google's repeated privacy

274. *See* STUCKE & GRUNES, *supra* note 40, at 164–65, 295; Mark Gurman, *7 Ways Google's Digital Assistant is Hobbled on Apple's iPhone*, AUSTRALIAN FIN. REV. (May 19, 2017, 10:18 AM), http://www.afr.com/technology/mobiles-and-tablets/apple/7-ways-googles-digital-assistant-is-hobbled-on-apples-iphone-20170518-gw8cef.

275. *See* STUCKE & GRUNES, *supra* note 40, at 295–96.

276. *See id.* at 295.

277. *See* Janice M. Mueller, *Patent Misuse Through the Capture of Industry Standards*, 17 BERKELEY TECH. L.J. 623, 633 (2002) (describing the anticompetitive effects of restricting digital assistant interoperability).

violations,[278] there has not been a mass exodus to rival search engines. Few people use multiple search engines (even though it very easy to multi–home).[279] When the search engine yields results that are not directly responsive to their query, most people attempt a different search query, rather than a different search engine.[280] If virtuous search engines, such as DuckDuckGo, have not prevented the abuses of the dominant search engine, we remain doubtful that a virtuous digital assistant (by DuckDuckGo or others) will fare any better.[281] If most users do not multi–home search engines, it is less likely they will train new digital assistants. Consequently, the combination of network effects, data, and the scope of the super–platform's services will likely lead one or two dominant digital assistants—either belonging to Google, Apple, Facebook, or Amazon.

V. POSSIBLE INTERVENTION

Though this Article focuses heavily on competition, the problems we identify reach beyond antitrust and so do the possible solutions. As any solution will depend on which digital assistants become dominant, their abuses, and the state of antitrust and privacy law and enforcement. When considering possible solutions, however, one can divide the solutions into two groups: First, a case–specific ex–post approach, which is reactive by nature. Second, an ex–ante approach, which focuses on changes to the regulatory or market framework. This Part briefly explore these two approaches.

To begin, an ex–post approach may lead to intervention when the platform operating the digital assistant holds a dominant position and abuses it. To establish dominance, market power must be sustained over time. It is important to stress that any form of ex–post intervention will have to be carefully measured to avoid chilling innovation and investment. Interventions will have to balance the benefits which flow from advanced technology and artificial intelligence against the welfare risks identified above.

278. *See* STUCKE & GRUNES, *supra* note 40, at 61–65.

279. Ezrachi & Stucke, *supra* note 120, at 490 n.37.

280. Amy Gesenhues, *Study: Top Reason a User Would Block a Site from a Search? Too Many Ads*, SEARCH ENGINE LAND (Apr. 15, 2013, 1:42 PM), http://searchengineland.com/?p=155708.

281. For a review of the possible ways in which algorithms could promote customer welfare, see Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J.L. & TECH. 309 (2017).

There are several difficulties with applying an ex–post approach to evaluate abuses by digital assistants. Regulators will have to evaluate whether the incumbent can operate independent of competitors and consumers; whether network effects and switching costs shield it from competitive pressure and establish dominance; and if dominance has been established, whether that position of dominance has been abused.

One noteworthy challenge concerns the dynamic of competition in markets in which services are offered for "free." Competition officials often adopt a price–centric approach to assess market power, namely whether the firm can charge supracompetitive prices. Rarely do they assess market power primarily in the form of non–price effects such as quality.[282] Another challenge concerns the weight regulators should attribute to disruptive innovation, which may suffice to ensure that the incumbents refrain from abusing their gatekeeper position.

Abuse may be established when the dominant undertaking engages in exclusionary, predatory or, in the EU, exploitative conduct.[283] Such strategies have attracted the European Commission's scrutiny in the past in the area of operating systems and search engines. In *Microsoft*,[284] the Commission was concerned with the leveraging of market power from the operating systems when Microsoft bundled Windows Media Player[285] and restricted interoperability with a view towards encouraging use of only Windows PCs with Microsoft group servers, thus discouraging investment

282. *See generally* STUCKE & GRUNES, *supra* note 40, at 107–26 (exploring non–price forms of market power in greater detail); Ariel Ezrachi & Maurice E. Stucke, *The Curious Case of Competition and Quality*, 3 J. ANTITRUST ENFORCEMENT 227 (2015).

283. *See, e.g.*, United States v. Grinnell Corp., 384 U.S. 563, 570–71 (1966) (holding that the offense of monopolization under Section 2 of the Sherman Act requires proof of "(1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident"); J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Wading Into Pandora's Box: Thoughts On Unanswered Questions Concerning The Scope And Application Of Section 2 & Some Further Observations On Section 5, Remarks at the LECG Newport Summit on Antitrust Law & Economics 1 (Oct. 3, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/wading-pandoras-box-thoughts-unanswered-questions-concerning-scope-and-application-section-2-some/091003roschlecgspeech.pdf.

284. Commission Decision, Case 37.792—Microsoft, C(2004) 900; Case T-201/04, Microsoft Corp. v. Comm'n, 2007 E.C.R. II-3601 (rejecting Microsoft's appeal of the commission's decision).

285. Commission Decision, Case 37.792—Microsoft, C(2004) 900, ¶ 826–34; *Microsoft*, 2007 E.C.R. II-3601 ¶ 856.

in non–Microsoft group servers.[286] Relatedly, in its Google investigation, the Commission raised concerns as to search degradation by Google and possible leveraging of market power.[287] In the case of digital helpers, of concern may be the super–platform's ability to favor its own services downstream and push out "as efficient" service providers (exclusionary abuse), or the ability to engage in price discrimination and extracting welfare from users (exploitative abuse). Intervention in such cases will bring the abuse to an end, and may include measure aimed at insuring access to the interface and better interoperability of platforms. At the extreme, when faced with a dominant platform which downgrades interoperability of others, one could consider forced access to the dominant firm's APIs.[288]

But the ex post approach has its shortcomings. First the agencies and courts may question the market power of digital assistants and their ability to behave independently of others.

Even if customers are locked in, one may have difficulties establishing some forms of abuse. The personalization of the service may make it difficult to ascertain an objective benchmark for comparison. For example, the European Commission alleged that Google favored its own comparison shopping service over those of competitors; users—to their detriment—did "not necessarily see the most relevant results in response to queries."[289] Inherent in this observation are several assumptions: (i) Google's organic or natural algorithm ordinarily provides objective results that most people would find relevant, (ii) Google manipulated the rankings of its organic search engine to systematically position and prominently display its comparison shopping service in its general search results pages, irrespective of its merits, and (iii) a remedy exists, namely enabling the organic algorithm—without interference—to treat Google's own comparison

286. Commission Decision, Case 37.792—Microsoft, C(2004) 900, ¶ 642–46; *Microsoft*, 2007 E.C.R. II-3601 ¶ 651.

287. Press Release, *supra* note 40.

288. For illustration, consider the theory of harm and remedy in Case T-201/04, Microsoft Corp. v. Comm'n, 2007 E.C.R. II-3601, where Microsoft was found to infringe Article 102 of the Treaty on the Functioning of the European Union because it refused to supply interoperability information to its competitors. *See also* Case C-418/01, IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG, 2004 E.C.R. I-5039; EUROPEAN COMM'N STRATEGY CENT., ENTER THE DATA ECONOMY (2017), https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_21.pdf.

289. Press Release, European Comm'n, Antitrust: Commission Takes Further Steps in Investigations Alleging Google's Comparison Shopping and Advertising-Related Practices Breach EU Rules (July 14, 2016), http://europa.eu/rapid/press-release_IP-16-2532_en.htm.

shopping service and those of rivals in the same way (namely no bias in favor of Google). Thus, the Commission could prove Google's intentional degradation with a ready counterfactual, namely what Google's own "organic" algorithm would have ranked as relevant, absent the manipulation.

But for a personalized search engine, tailored to each individual's particular tastes, credible counterfactuals to quality degradation may be difficult to establish. There may not be an organic algorithm. Nor is there an objective baseline for "Alexa, what's the latest on Donald Trump?" If Alexa provides a *Washington Post* story (which Amazon's CEO owns), it may be difficult to assess whether this is evidence of quality degradation. What interests conservatives may not interest liberals.[290] Even if the topic is of interest, the user might desire a particular viewpoint.[291] Thus, it will likely be harder to prove search degradation for a *personalized* digital assistant than for a *general* search engine.[292] As the primary interaction takes place at the personal–assistant level, the effects may be seen more as personalization (and thus a legitimate part of technological progress) than exclusionary.

Third is the political will to challenge monopolization cases. In contrast to the European Commission, the U.S. Department of Justice and Federal Trade Commission have not meaningfully prosecuted monopolistic abuses over the past few decades. The DOJ criminally prosecuted more persons in one year under the Migratory Bird Treaty Act (227 in 2012) than it has civilly and criminally prosecuted monopolies over the past 35 years (13 since 1980).[293] Between 2007 and 2016, the DOJ opened seventeen monopolization investigations, and brought only one case (in 2011).[294]

Beyond the traditional ex-post application of antitrust law, one may identify a range of instruments which could be used, ex ante, to support consumer welfare. Ex ante measures—implemented through sector investigations, agreed commitments, regulatory instruments. or consumer protection laws—may be used to require compliance with preconditions to promote privacy competition, ensure that the platform's incentives are aligned with users' interests, and prevent some of the market dynamics which could give rise to exclusionary or exploitative effects.

290. *See* Bakshy et al., *supra* note 149, at 1130–31.
291. *See id.*
292. ECONOMIST, *supra* note 117.
293. STUCKE & GRUNES, *supra* note 40, at 300.
294. *Id.*; DEPT. OF JUSTICE, ANTITRUST DIVISION WORKLOAD STATISTICS FY 2007–2016 at 1, 5 (2017), https://www.justice.gov/atr/division-operations.

For instance, basic measures would ensure that users retain autonomy, are made aware of outside options and can switch with limited or no costs. One could require digital assistants to indicate clearly, either in a pop–up window or voice warning when their suggestions are "sponsored" or when they offer service through their own platform network while excluding others. Users may be able to opt out of personalized ads or sponsored products.[295] All these measures, to be effective, require short and clear communications. Often the consent in today's click–wrap is little more than a façade.[296] Knowing and voluntary consent is key. When users have few, if any, viable options, consent is not real but forced.[297] In addition, "consent fatigue" or digital helpers managing consent forms on their users' behalf, could lead to meaningless agreement and undermine customer empowerment.[298]

To allow switching between digital assistants, regulators and policymakers should encourage data mobility. One proposal in Europe is a "Personal Information Management System," which collects and stores the user's data:

> With PIMS, users would have a personal digital deck where all their information is stored. Services (such as Facebook) would then run on this deck, giving users the ability to keep track and control the information they share and, above all, easily use that information for multiple platforms. Hence, PIMS have the potential to significantly increase transparency and portability of data and, therefore stimulate data service competition.[299]

With adequate safeguards one should be able to transfer the core parameters, which will enable a new digital assistant to start from a position of personalization. At the providers' side, mobility would require access to platforms and the provision of interoperability information. Mobility may require the development of basic industry standards for key data points and will need to take into account issues of licensing and IP rights. Their development should nonetheless allow sufficient freedom for developers, to enable disruptive innovation.

---

295. Transparency is key—for example, in a 2017 update, Google allowed users to opt out of personalized ads. Ryan Whitwam, *How to Disable Personalized Ads on Android*, FORBES (Mar. 31, 2017, 11:56 AM) https://www.forbes.com/sites/ryanwhitwam/2017/03/31/how-to-disable-personalized-ads-on-android/. This is a positive move, which ensures user control over his or her data and search environment.

296. STUCKE & GRUNES, *supra* note 40, at ch. 21.

297. *Id.* at 58–66.

298. EZRACHI & STUCKE, *supra* note 2, at 226.

299. *Id.* at 12.

VI. CONCLUSION

In industries dominated with data–driven network effects, consumers will likely receive free digital assistants. These assistants will excel at mundane tasks—and as AI develops—they will increasingly assist users with their daily tasks. Seeing the salient, day–to–day benefits, users may trust and rely on their digital assistant. The assistant will no longer be simply making French press coffee and turning on the lights in the kids' rooms. It will be tutoring children, entertaining families, telling happy or sad stories from around the world, ordering food (and the books that it recommends), and summoning the driverless car to whisk people to work.

As consumers welcome digital assistants into their homes, they may not recognize their toll on our well–being. It is often hard to quantify long–term costs and balance these against short–term gains. Digital assistants may be helpful, no doubt. As the digital assistant increasingly controls mundane household tasks, like regulating room temperature and playing music, it will be harder to turn off. It will also be tempting to increasingly rely on the digital assistant for other activities, such as receiving news, selecting shows to watch, and identifying goods to buy. But consumers should be mindful about the power they may have on data gathering and distribution and the subsequent implications for privacy and our welfare.

Policymakers cannot assume that market forces will deliver the virtuous assistant or curb the abuses described in this Article. Market forces, given data–driven network effects, have the potential to increase entry barriers, make the strong platforms (and their digital assistants) even stronger, and weaken many independent digital assistants. These assistants would assist in consolidating economic and political power into fewer hands. Market forces, left unchecked, may yield a dominant and devious digital assistant even though the technology exists for an independent virtuous assistant. The large platform could extract even more personal data and command even higher rents to allow other corporations to reach consumers. Not only will consumer wallets be affected, but super–platforms could also manipulate political and social discourse. These privacy, economic, and political concerns will increase when the digital assistant is connected not only to television sets, but computers, smart appliances, security cameras, smartphones, and smart cars.

In sum, while it is easier to see the immediate benefits from these digital assistants, understanding the long–term risks—while harder to see—is key. No one likes a snooping digital assistant, especially one that profits at the expense of innocent consumers. As this Article has described, super–platforms and their digital assistants present unique challenges. Regulators

and legislators must take steps to minimize the risks and protect consumers interests and freedom. This is not a campaign against innovation, nor is it a call for unconstrained state intervention. Rather, we should ask for a balanced policy—one which promotes competition and innovation and most importantly, social welfare. In a nutshell, the goals for a data–driven economy should be an economy that's inclusive, protects the privacy interests of its citizens, promotes the citizenry's overall wellbeing, and also promotes a healthy democracy.