EDITOR'S NOTE

Welcome to the second Issue of Volume 73 of the *Federal Communications Law Journal*, the nation's premier communications law journal and the official journal of the Federal Communications Bar Association (FCBA). This Issue showcases the breadth of scholarship in telecommunications and technology law, spanning from broadband regulation to information privacy to the regulation of e-commerce.

This Issue begins with an article authored by Jonathan E. Nuechterlein and Howard Shelanski examining proposed broadband regulation, ultimately cautioning that the proposals fail to identify real market failures and are too costly. Nuechterlein and Shelanski argue that the government can address real market problems, such as digital divides by expanding targeted subsidy mechanisms.

This Issue also features four student Notes. In the first Note, Hunter Iannucci illustrates the inability of current legal mechanisms to protect the informational privacy rights of transgender public figures. Iannucci argues that the European Union's right to be forgotten law can be constitutionally replicated in the U.S. to allow transgender public figures to remove online information about themselves inconsistent with their gender identities. In the second Note, Olivia T. Creser addresses consumer harm online and the now common call to break up Big Tech. Creser provides a counterproposal, that Section 5 of the Federal Trade Commission Act can be amended to protect consumers. In the third Note, Brooke Rink discusses the online mugshot industry. Rink argues that Congress may act to limit the release of such images and that exploitative websites may be further regulated through a modification to Section 230. In the final Note, Shuyu Wang describes the challenge of regulating counterfeit merchandise sold through Chinese social media platforms. Wang proposes that those social media platforms with in-app shopping features fall under the regulation of e-commerce platforms to allow better trademark enforcement in China, a model that could shed light on the recent U.S. proposal seeking to combat online counterfeits: the SHOP SAFE Act.

We thank the FCBA and The George Washington University Law School for their continued support. This Issue marks one year into the COVID-19 pandemic which posed unique challenges for the *Journal*, including the cancellation of our 3rd Annual Spring Symposium in 2020, but brought new opportunities, like our partnership with the Berkeley Center for Law & Technology for our joint virtual Spring Symposium in 2021. We thank our all our contributors for their work during this remarkable year.

The *Journal* is committed to providing its readership with rigorous academic scholarship and thought leadership in relevant topics in communications and information technology law. Please send submissions to be considered for publication to fcljarticles@law.gwu.edu. All other questions or comments may be directed to fclj@law.gwu.edu. This Issue and our archive are available at www.fclj.org.

Elissa C. Jeffers
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

VOLUME 73

Published by the GEORGE WASHINGTON UNIVERSITY LAW SCHOOL
and the FEDERAL COMMUNICATIONS BAR ASSOCIATION

Federal Communications Law Journal

The *Federal Communications Law Journal* is published jointly by the Federal Communications Bar Association (FCBA) and The George Washington University Law School. The *Journal* publishes three issues per year and features articles, student notes, essays, and book reviews on issues in telecommunications, the First Amendment, broadcasting, telephony, computers, Internet, intellectual property, mass media, privacy, communications and information policymaking, and other related fields.

As the official journal of the FCBA, the *Journal* is distributed to over 2,000 subscribers, including Association members as well as legal practitioners, industry experts, government officials and academics. The *Journal* is also distributed by Westlaw, Lexis, William S. Hein, and Bloomberg Law and is available on the Internet at www.fclj.org.

The *Journal* is managed by a student Editorial Board, in cooperation with the Editorial Advisory Board of the FCBA and two Faculty Advisors.

Federal Communications Bar Association

The FCBA (d/b/a FCBA – The Tech Bar) is a volunteer organization of attorneys, engineers, consultants, economists, government officials and law students involved in the study, development, interpretation and practice of communications and information technology law and policy. From broadband deployment to broadcast content, from emerging wireless technologies to emergency communications, from spectrum allocations to satellite broadcasting, the FCBA has something to offer nearly everyone involved in the technology, media, and telecommunications industries. That's why the FCBA, more than two thousand members strong, has been the leading organization for communications lawyers and other professionals since 1936.

Through its many professional, social, and educational activities, the FCBA offers its members unique opportunities to interact with their peers and decision-makers in the communications and information technology field, and to keep abreast of significant developments relating to legal, engineering, and policy issues. Through its work with other specialized associations, the FCBA also affords its members opportunities to associate with a broad and diverse cross-section of other professionals in related fields. Although the majority of FCBA members practice in the metropolitan Washington, DC area, the FCBA has 11 active regional chapters, including: Atlanta, Carolina, Florida, Midwest, New England, New York, Northern California, Southern California, Pacific Northwest, Rocky Mountain, and Texas. The FCBA has members from across the U.S., its territories, and several other countries.

The George Washington University Law School

Established in 1865, The George Washington University Law School (GW Law) is the oldest law school in Washington, DC. The Law School is accredited by the American Bar Association and is a charter member of the Association of American Law Schools. GW Law has one of the largest curricula of any law school in the nation with more than 275 elective courses covering every aspect of legal study.

GW Law's home institution, The George Washington University is a private institution founded in 1821 by charter of Congress. The Law School is located on the University's campus in the downtown neighborhood familiarly known as Foggy Bottom.

The *Federal Communications Law Journal* is published by The George Washington University Law School and the FCBA three times per year. Offices are located at 2028 G Street NW, Suite LL-020, Washington, DC 20052. The *Journal* can be reached at fclj@law.gwu.edu, and any submissions for publication consideration may be directed to fcljarticles@law.gwu.edu. Address all correspondence with the FCBA to FCBA, 1020 19th Street NW, Suite 325, Washington, DC 20036-6101.

Subscriptions: Subscriptions are $30 per year (domestic), $40 per year (Canada and Mexico), and $50 per year (international). Subscriptions are to be paid in US dollars, and are only accepted on a per-volume basis, starting with the first issue. All subscriptions will be automatically renewed unless the subscriber provides timely notice of cancellation. Address changes must be made at least one month before publication date, and please provide the old address or an old mailing label. Please direct all requests for address changes or other subscription-related questions to the journal via email at fclj@law.gwu.edu.

Single and Back Issues: Each issue of the current volume can be purchased for $15 (domestic, Canada and Mexico) or $20 (international), paid in U.S. dollars. Please send all requests for single or back issues to fclj@law.gwu.edu.

Manuscripts: The *Journal* invites the submission of unsolicited articles, comments, essays, and book reviews mailed to the office or emailed to fcljarticles@law.gwu.edu. Manuscripts cannot be returned unless a self-addressed, postage-paid envelope is submitted with the manuscript.

Production: The citations in the *Journal* conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia L. Rev. Ass'n et al. eds., 21st ed., 2020). Variations exist for purposes of clarity and at the editors' discretion. The *Journal* is printed by Joe Christensen, Inc.

Citation: Please cite this issue as 73 FED. COMM. L.J. 2 (2021).

FEDERAL COMMUNICATIONS LAW JOURNAL

GW LAW

VOLUME 73 ISSUE 2

FEBRUARY 2021

FCBA FEDERAL COMMUNICATIONS BAR ASSOCIATION

ARTICLE

Building on What Works: An Analysis of U.S. Broadband Policy

Issued ten years ago, the FCC's National Broadband Plan was in many respects a case study in regulatory humility. It recognized that broadband progress was "[f]ueled primarily by private sector investment and innovation"; that "government cannot predict the future"; that "the role of government is and should remain limited"; and that policymakers should thus focus not on imposing price controls or behavioral restrictions, but on "encourag[ing] more private innovation and investment." This advice, which the FCC has generally followed, has fared well under the test of time. Ten years and hundreds of billions of investment dollars later, the broadband marketplace now offers consumers more choices and exponentially faster speeds than it did then.

Against that backdrop, this paper analyzes the asserted need for, and likely consequences of, four types of broadband regulation proposals in recent circulation: (1) facilities-sharing obligations; (2) retail price controls; (3) internet interconnection obligations; and (4) amorphous and open-ended ISP conduct rules like those the FCC imposed in 2015. For the most part, we see little merit to any of these proposals under current market conditions. None of them is needed to address any identifiable market failure, and each would impose significant costs, including the investment-chilling prospect of regulatory creep.

That said, government retains a critical role to play in the broadband marketplace. Market forces are unmatched in their power to bring the greatest benefit to the greatest number. But market forces by themselves will not help America close two stubborn and unacceptable digital divides: between rich and poor, and between urban and rural. These are real, universally acknowledged problems that call for real solutions. In particular, they call for expanded subsidy mechanisms—one directed to low-income subscribers and the other to broadband providers that commit to new infrastructure deployment in rural and other high-cost areas. But the challenge of closing these digital divides does not even logically support a call for more intrusive regulation of the broadband industry. To the contrary, such regulation would, if anything, make the underlying problems worse by placing a thumb on the scale against additional broadband investment.

NOTES

Building on What Works: An Analysis of U.S. Broadband Policy

Jonathan E. Nuechterlein*
Howard Shelanski

TABLE OF CONTENTS

* Jonathan Nuechterlein is partner at Sidley Austin LLP and previously served as General Counsel of the FTC (2013-16) and Deputy General Counsel of the FCC (2000-01). Howard Shelanski is Professor of Law at Georgetown University and partner at Davis Polk & Wardwell LLP. He previously served as Administrator of the Office for Information and Regulatory Affairs (2013-17), Director of the FTC's Bureau of Economics (2012-13), Chief Economist of the FCC (1999-2000), and Senior Economist for the President's Council of Economic Advisors (1998-99). Over the course of our careers, we have represented both the federal government and broadband providers on issues relevant to this article, and we gratefully acknowledge the support of USTelecom–The Broadband Association and NCTA–The Internet and Television Association in funding this research. All views expressed here are our own and do not necessarily reflect the views of USTelecom, NCTA, or their members.

I. INTRODUCTION AND SUMMARY

This year marks three milestones in telecom policy. Each conveys an important lesson for policymakers as they contemplate broadband regulation for the 2020s and beyond.

First, it has been ten years since the Obama FCC released the *National Broadband Plan*, which surveyed the U.S. broadband landscape in 2010 and offered policy recommendations for boosting deployment and adoption. In many respects, the *Broadband Plan* was a case study in regulatory humility. It recognized that broadband progress was "[f]ueled primarily by private sector investment and innovation"; that "government cannot predict the future"; that "the role of government is and should remain limited"; and that policymakers should thus focus not on imposing price controls or behavioral restrictions, but on "encourag[ing] more private innovation and investment."[1] This advice, which the FCC has generally followed, has fared well under the test of time. Ten years and hundreds of billions of investment dollars later, the broadband marketplace now offers consumers more choices and exponentially faster speeds than it did then. The *Plan* was also eerily prescient. In one passage, it anticipated "surge[s] in residential broadband network use during a pandemic" and the need for "high standards of reliability, resiliency and security."[2] Those are standards that U.S. networks have more than met during the COVID-19 pandemic, as broadband usage has surged.[3]

Second, it has been twenty years since the FCC issued the 2000 *Notice of Inquiry* seeking comment for the first time on "the appropriate legal classification of cable modem service" and "what regulatory treatment, if any, should be accorded" to it.[4] As the *NOI* noted, the FCC had consistently "taken a 'hands-off' policy" for cable broadband services,[5] then the dominant form

1. FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN, at XI, 5 (2010) (hereinafter *National Broadband Plan* or *Plan*).

2. *Id.* at 313, 322.

3. *See* Tyler Cooper, *Internet Performance Around the World Amid COVID-19*, BROADBANDNOW (May 6, 2020), https://broadbandnow.com/report/international-internet-performance/ [https://perma.cc/HB8Z-MWP4] ("Of the top 10 countries in the world by population, the U.S. is the only that recorded no download speed degradation on average in the month of April."); *SamKnows Critical Services Report: Fixed Speed (USA)*, SAMKNOWS (Apr. 14, 2020), https://samknows.com/blog/samknows-critical-services-report-fixed-speed-usa [https://perma.cc/RGE4-4SNM] ("Broadband infrastructure in the US is holding up generally very well given the dramatic increase in internet usage."); *see also* Roger Entner, *Industry Voices – Entner: A Tale of Two Continents and the Internet During COVID-19*, FIERCE TELECOMM. (Apr. 29, 2020), https://www.fiercetelecom.com/telecom/industry-voices-entner-a-tale-two-continents-and-internet-during-covid-19 [https://perma.cc/F88Z-XZXK]; Doug Brake, *Lessons From the Pandemic: Broadband Policy After COVID-19*, INFO. TECH. & INNOVATION FOUND'N (July 2020), https://itif.org/sites/default/files/2020-broadband-lessons-from-pandemic.pdf [https://perma.cc/B5LZ-7NH3].

4. Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, *Notice of Proposed Rulemaking*, 17 FCC Rcd 4798 (7), paras. 1, 5 (2000) [hereinafter *2000 FCC NOI*].

5. *Id.* ¶ 4; *see also* Section III.B.4, *infra*.

of broadband Internet access. The basis for that policy, which the FCC reaffirmed in later orders, was best summed up by then-FCC Chairman Bill Kennard, for whom we both worked at the end of the Clinton Administration. As he explained:

> We sometimes get so caught up in the policy debates about broadband . . . that we forget what we need to do to serve the American public. . . . *We have to get these pipes built. But how do we do it? We let the marketplace do it.* . . . [T]he best decision government ever made with respect to the Internet was the decision that the FCC made . . . NOT to impose regulation on it. This was not a dodge; it was a decision NOT to act. It was intentional restraint born of humility. Humility that we can't predict where this market is going.[6]

Twenty years later, private enterprise has invested more than a trillion dollars to "build the pipes." As a result, the typical American can now choose among multiple competing broadband services—both fixed-line and mobile—at speeds nearly unimaginable in 2000. And broadband ISPs made these investments against the backdrop of a light-touch regime that, with rare exceptions, declined to apply significant economic regulation for two decades. It is difficult to prove causal links between regulatory choices and specific investment decisions, but as a matter of economic logic, more intrusive forms of regulatory intervention would likely have reduced, not increased, incentives to commit private risk capital to broadband infrastructure and innovation.

Third, it has been 25 years since the House and Senate issued the bills that became the Telecommunications Act of 1996.[7] Much has been written about that legislation, both positive and negative. Among its undeniable achievements, the 1996 Act eliminated anticompetitive exclusive franchises, began rationalizing universal service mechanisms, and consolidated competition policy at the federal level at a time when technology had begun blurring the traditional distinctions between "intrastate" and "interstate" services.[8] But the 1996 Act is also notorious for launching years of unproductive regulatory churn, mainly surrounding the interventionist "unbundling" rules the FCC designed to mimic but not necessarily produce genuine facilities-based competition in landline telephone markets.[9] Those rules show how even the smartest regulators can do more harm than good if they underestimate prospects for facilities-based entry—in that case, the looming ascendance of mobile networks and VoIP technologies over the

6. William E. Kennard, Chairman, FCC, Remarks before the National Cable Television Association: The Road Not Taken: Building a Broadband Future for America (June 15, 1999) [hereinafter 1999 Kennard Remarks] (emphasis added), http://www.fcc.gov/Speeches/Kennard/spwek921.html [https://perma.cc/RJ6H-829F].

7. Pub. L. No. 104-104, 110 Stat. 56 [hereinafter *1996 Act*].

8. *See* AT&T Corp. v. Iowa Utils. Bd., 525 U.S. 366, 393–94 (1999).

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

landline telephone network—and overestimate the efficacy and administrability of complex regulatory obligations.

These three milestones should inform today's debates about broadband policy. The *National Broadband Plan* reflects the best traditions of the FCC's professional staff: focusing on the facts, recognizing the complexity of markets, and promoting policies that enhance rather than undermine private incentives for investment and innovation. Chairman Kennard's turn-of-the-milennium policy of "intentional restraint born of humility" reflects the same commitment to data-driven broadband policy. But the network-sharing regime adopted under the 1996 Act offers a more cautionary tale. It illustrates the costly detours that telecom policy can take when well-intentioned regulators pursue novel schemes of regulatory intervention on the mistaken assumption that markets would stagnate without them.

The broadband industry today is more technologically dynamic and competitive than the landline telephone industry of 1996, but the two share one similarity. Much like the turn-of-the-millennium telephony market, the broadband industry is in new period of technological transition. Fixed-line networks are deploying technologies that support increasingly mobile functionality, while mobile networks—first with LTE and now with 5G—are increasingly capable of cost-efficiently supporting high-bandwidth services that were once the unique province of fixed-line networks.[10] If experience with the 1996 Act taught us nothing else, it is that policymakers must be careful neither to exaggerate the need for major intervention in such transitional markets nor to overlook the costs of doing so.

Unfortunately, current proposals for market intervention are often long on rhetoric and short on real analysis of likely tradeoffs and actual consequences. This paper thus analyzes the asserted need for, and likely consequences of, four types of proposals in recent circulation: (1) facilities-sharing obligations, (2) retail price controls, (3) Internet interconnection obligations, and (4) amorphous and open-ended ISP conduct rules like those the FCC imposed on consumer broadband services in 2015.[11] For the most part, we see little merit to any of these proposals under current market conditions. None of them addresses any identifiable market failure and each would impose significant costs, including the investment-chilling prospect of regulatory creep. That said, we support re-imposition of bright-line prohibitions on blocking or throttling to guard against any risks to the Internet's status as an open, positive-externalities-generating platform for communication and innovation. Although those risks appear remote, such bright-line rules would reduce them to zero and impose minimal costs because

10. *See, e.g.*, *Wireless Strategies Beyond Wi-Fi for Fixed Network Service Providers*, BELL LABS CONSULTING (Apr. 26, 2016), https://media-bell-labs-com.s3.amazonaws.com/pages/20190111_1455/NokiaWirelessStrategiesBeyondWiFiforFixedNetworkServiceProviders.pdf [https://perma.cc/8WVT-JGJ5]; Don Reisinger, *Home Broadband Providers Face an Uncertain Future in the 5G Era*, FORTUNE (Feb. 13, 2020), https://fortune.com/2020/02/13/5g-impact-on-broadband/ [https://perma.cc/2H9G-Z52X].

11. *See generally* Protecting and Promoting the Open Internet, *Report & Order on Remand*, *Declaratory Rule, and Order*, 30 FCC Rcd. 5601 (2015).

such rules would simply codify what have become industry norms in any event.

All this said, government retains a critical role to play in the broadband marketplace. Market forces are unmatched in their power to bring the greatest benefit to the greatest number. But market forces by themselves will not help America close two stubborn and unacceptable digital divides: between rich and poor, and between urban and rural.[12] As the COVID-19 pandemic underscores, broadband is critical to equal opportunity and to full participation in civic and economic life, but underemployment has made it unaffordable for many Americans. At the same time, many Americans in rural areas cannot buy the connectivity they need at any price. The great broadband challenge of the next decade is to close both divides by boosting *adoption* in low-income communities and *deployment* in high-cost areas.

These are real, universally acknowledged problems that call for real solutions. In particular, they call for expanded subsidy mechanisms—one directed to low-income subscribers and the other to broadband providers that commit to new infrastructure deployment in rural and other high-cost areas. But the challenge of closing these digital divides does not even logically support a call for more intrusive regulation of the broadband industry. To the contrary, such regulation would, if anything, make the underlying problems worse by placing a thumb on the scale against additional broadband investment.

* * *

This paper is divided into three main sections. Section II addresses the types of market conditions that do—and do not—call for economic regulation, the focus of this paper. By "economic regulation," we mean rules intended to constrain the exercise of market power (*e.g.*, retail rate caps) or force firms to cooperate with other firms, including their rivals (*e.g.*, asset-sharing, interconnection, and "neutrality" obligations).[13] As we discuss, a rigorous analysis of tradeoffs and consequences generally disfavors economic regulation in industries that, like broadband, are technologically dynamic and subject to competition. Section III then summarizes the history of light-touch broadband regulation in the U.S. before critiquing proposals for major

12. *See* Monica Anderson & Madhumitha Kumar, *Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption*, PEW RES. CTR. (May 7, 2019), https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/ [https://perma.cc/Z6NP-L6UQ]; Andrew Perrin, *Digital Gap Between Rural and Nonrural America Persists*, PEW RES. CTR. (May 31, 2019), https://www.pewresearch.org/fact-tank/2019/05/31/digital-gap-between-rural-and-nonrural-america-persists/ [https://perma.cc/P2VY-APCS].

13. Of course, telecommunications firms face many other types of regulation, including obligations relating to consumer privacy, truth in billing, network-management disclosures, and spectrum usage as well as conditions placed on participation in discretionary funding programs. This paper focuses on economic regulation, not these other types of market intervention.

intervention. Finally, Section IV addresses the imperative to reconcile competition policy with the demands of social equity.

II. THE COMPETITIVE DYNAMICS OF THE U.S. BROADBAND MARKETPLACE

Most markets, including very concentrated ones, are not subject to economic regulation at all.[14] For example, the government does not regulate prices for iPhones, Microsoft Word, Intel microprocessors, or most pharmaceuticals. Nor, apart from the occasional antitrust case, does the government otherwise subject such products to economic regulation.

Instead, the government typically reserves such regulation for mature markets that are dominated by durable monopolies, lack serious prospects for competitive entry, and are subject to only gradual changes in technology or consumer demand. Quintessential examples include the electric power distribution market and the wireline telephone industry of the mid-20th century.[15] In such settings, the cost-benefit calculus often tips sharply in favor of regulatory intervention. Absent regulation, the enduring lack of competition almost certainly pushes prices far above costs (however measured), with accompanying deadweight losses. The *benefits* of regulation in this scenario are straightforward: although a regulator may never be able to get prices exactly "right"—in the sense of replicating price levels in a genuinely competitive market—the regulator is likely to set prices closer to efficient levels than they would otherwise be.[16]

At the same time, the *costs* of imposing regulation on a stable monopoly market are low because by hypothesis, technological change is slow and the odds of competitive entry are slim. To see this point, consider the downside risks of regulation in markets characterized by actual or potential competition. In such markets, price regulation lowers profit margins for potential entrants because in order to win business, they must now undersell not the prices that an unregulated monopolist would have charged, but the substantially lower prices set by regulators. That revenue differential will obviously affect the risk-reward calculus for a potential entrant and, in some cases, may deter entry altogether. But in markets where competitive entry is unlikely, the incremental harm from forgone competition is small by hypothesis. Likewise, in highly stable markets where technological disruption is unlikely anyway, the entry-deterring effects of regulation will probably cause little or no incremental harm to innovation.

For the same reasons, where markets *are* subject to competition or at least a real prospect of competitive entry, the cost-benefit analysis points in the opposite direction.[17] Because competition by definition moves prices

14. *See* Howard A. Shelanski, *Adjusting Regulation to Competition: Toward a New Model for U.S. Telecommunications Policy*, 24 YALE J. REG. 55, 64–65 (2007).

15. *See* JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: TELECOMMUNICATIONS LAW AND POLICY IN THE INTERNET AGE 10–12, 32–35 (2d ed. 2013).

16. Shelanski, *supra* note 14, at 84.

17. *Id.* at 77–84.

closer to competitive levels, and because regulators are not omniscient, regulation is less likely to set prices more efficiently than market forces, and even when it does, the improvement will be smaller in magnitude. And as noted, economic regulation runs a greater risk of doing affirmative harm when applied to a potentially competitive market; because by lowering expected returns on investment, it makes competitive entry or expansion less attractive to a potential entrant than it otherwise would be and it blunts the incentives of incumbents to make risky investments of their own.[18]

As a general matter, the U.S. broadband industry falls into the category of competitive markets, for which economic regulation is normally inappropriate, rather than the category of technologically static monopolies, for which such regulation is often necessary. To begin with, broadband markets in the U.S. are generally not monopolistic. As discussed below, most consumers can choose among at least two competing providers of fixed-line broadband services, quite apart from their mobile broadband options.[19] Indeed, fixed-line broadband markets in this country are often substantially more competitive—in the sense of featuring multiple facilities-based rivals—than those of comparable industrialized nations. As the *National Broadband Plan* recognized in 2010, "the U.S. market structure is relatively unique" in that "many countries have a single, dominant nationwide fixed telecommunications provider," whereas "the United States has numerous providers," including cable companies, which "play a more prominent role in our broadband system than in other countries."[20]

This feature of U.S. broadband markets stems from the early days of cable television, which has generally been more popular in the U.S. than abroad. In many OECD nations, residential broadband in most areas has long been provided over a single landline network owned and operated by legacy telephone monopolists, often state-owned or state-supported.[21] In contrast, cable television companies in the U.S. (most of them privately owned) grew up independently of the major telephone companies (which also have been privately owned for the most part).[22] U.S. cable companies enjoyed extraordinary success over the ensuing decades, in part because Americans are uniquely voracious consumers of television programming. Cable companies had thus deployed high-bandwidth transmission infrastructure throughout much of America by the time broadband took root at the turn of the 21st century.[23] Indeed, cable companies were generally the first home broadband providers out of the gate.[24] Legacy telephone companies had to play catch-up to match the speeds of their cable competitors, whose transmission pipes were fatter because they were originally designed to carry

18. *Id.* at 81–82.
19. *See infra* note 34 and accompanying text.
20. *National Broadband Plan*, *supra* note 2, at 4, 37.
21. *Id.* at 4.
22. *See History of Cable*, CAL. CABLE & TELECOMMS. ASS'N, https://calcable.org/learn/history-of-cable/ (last visited Dec. 1, 2020) [https://perma.cc/Q4S5-CGUW].
23. *National Broadband Plan*, *supra* note 2, at 37.
24. *See* Nuechterlein & Weiser, supra note 15, at 192.

high-bandwidth television programming rather than low-bandwidth voice calls.[25]

Advocates for greater regulation have contended at various points over the past twenty years that these early advantages would make cable an enduring monopoly and that legacy telcos, supposedly unable to hold their own, would fade as broadband competitors.[26] But the facts have not borne out that prediction, which becomes less credible each time it is repeated. Consider the Open Technology Institute's prediction in 2012 that consumers "will likely face a near-monopoly from cable providers" and that this "erosion in competition" was "likely to reduce incentives for cable providers to upgrade their infrastructure to offer higher speeds."[27] OTI was right about one thing: if cable companies *were* natural monopolists and could thus rest easy, one would not expect to see them and other ISPs making enormous continuing investments in major facilities upgrades to improve service levels year after year, for that is a hallmark of competitive markets. But that is what we *do* see, contrary to OTI's prediction.

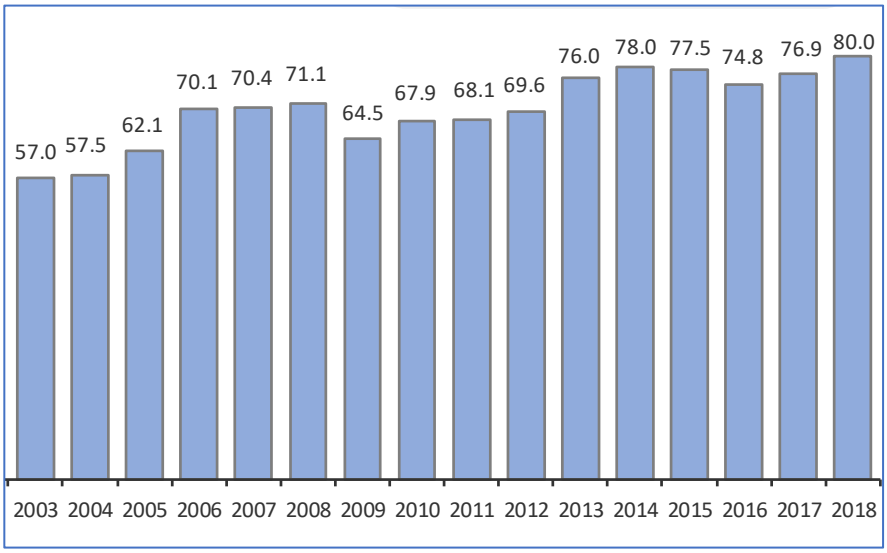
In particular, broadband providers have collectively invested more than $1.7 *trillion* since 1996—and more than $70 billion each year since 2013—to keep pace with their competitors and meet consumer demand for ever-increasing speeds:

25. *Id.*

26. *E.g.*, Christopher Jon Sprigman, *Net Neutrality Is Great, but It Won't Make Broadband Cheaper*, NEW YORKER (June 21, 2016), https://www.newyorker.com/business/currency/net-neutrality-is-great-but-it-wont-make-broadband-cheaper [https://perma.cc/E3KT-5MGJ] (proposing "local-loop unbundling" to address the "monopoly power" of cable companies); Susan P. Crawford, *The Communications Crisis in America*, 5 HARV. L. & POL'Y REV. 245, 248, 261 (2011) ("Given the tremendous economies of scale and cost advantages of the cable industry, being a wireline phone company is not a great business these days. . . . The emergence of a de facto cable monopoly in high-speed wired Internet access in most of the country cannot stay a secret.").

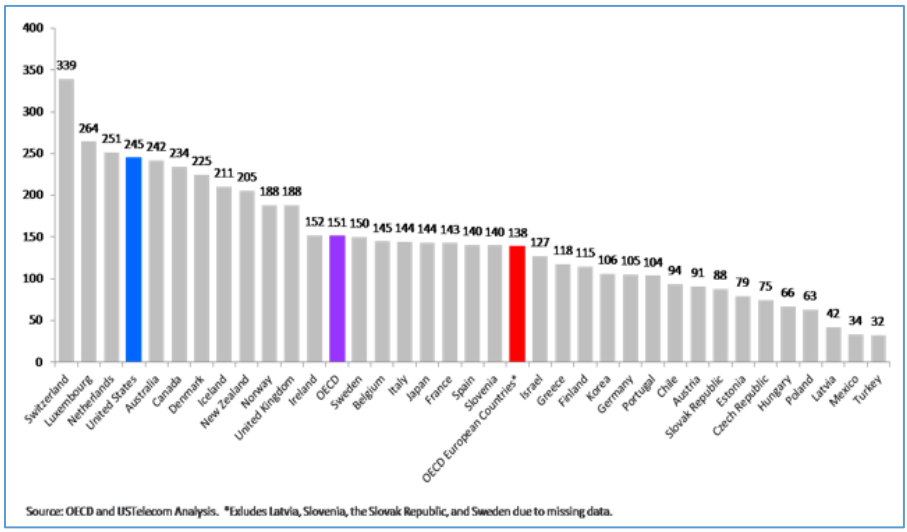
27. Hibah Hussain et al., Open Tech. Inst., New Am. Found., *The Cost of Connectivity* 10–11 (July 2012), https://d1y8sb8igg2f8e.cloudfront.net/documents/the-cost-of-connectivity-2012.pdf [https://perma.cc/QU87-KN5F].

U.S. Fixed and Mobile Broadband Capital Expenditures ($ billions)[28]



These numbers are large not only in absolute terms, but also when compared to foreign per-capita investment figures:

Average Annual Telecom Capital Investment Per Capita 2003-2015 (USD)[29]



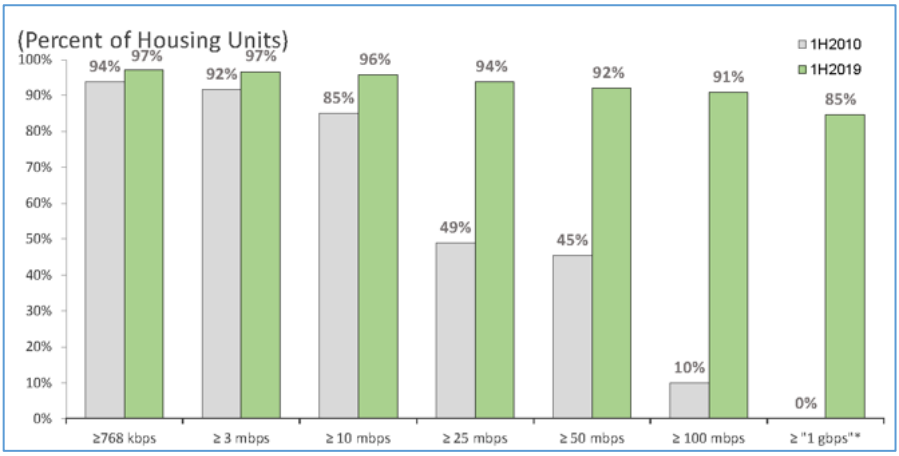
Broadband providers have made these continuing investments because they know that they face competition and must deliver ever-improving service

28. *USTelecom Industry Metrics & Trends 2020*, USTELECOM 7 (Apr. 2020), https://www.ustelecom.org/wp-content/uploads/2020/04/USTelecom-State-of-Industry-2020-Update.pptx [https://perma.cc/EYR6-E4SW].

29. *Id.* at 9.

to win and retain customers. Again, the numbers tell the story. The fixed broadband speeds available to the typical American household have skyrocketed over the past 10 years, as high-bandwidth applications such as streaming video and videoconferencing have surged in popularity:

Broadband Availability by Download Speed for Wired Technologies 2010-2019[30]



And as broadband speeds soar, the average price per unit of consumption continues to plummet. According to one industry estimate, consumers in 2018 paid on average about $0.76 per Mbps—a 92% decrease from the $9.01 per Mbps they paid on average in 2008.[31]

The available direct statistics on competition, while imperfect,[32] reaffirm that most American households can also choose among multiple fixed broadband providers. According to official FCC data, about 70% of the U.S. population lives in census blocks where two or more fixed providers

30. *Id.* at 15.

31. *The Shrinking Cost of a Megabit*, NCTA (Mar. 28, 2019), https://www.ncta.com/whats-new/the-shrinking-cost-of-a-megabit [https://perma.cc/4RC7-N22U]; *see also Industry Data*, NCTA, https://www.ncta.com/industry-data (last visited Sept. 20, 2020) [https://perma.cc/P254-FCCG] ("The price per Mbps has declined [98%] from an average of $28.13 in 2000 to $0.64 in 2020."); Arthur Menko, *2020 Broadband Pricing Index*, USTELECOM (2020) https://www.ustelecom.org/wp-content/uploads/2020/09/USTelecom-2020-Broadband-Pricing-Index.pdf [https://perma.cc/YPY3-BXZT] (finding that, between 2015 and 2020, the real price per Mbps fell 56.1% for the fastest residential broadband speed tier and 37.9% for the most popular speed tier).

32. For many years, the FCC has required fixed-line broadband providers to report the census blocks in which they offer broadband services. The problem is that census blocks, while small in urban areas, can be very large in rural areas, and the fact that an ISP offers broadband in one part of a large census block does not necessarily mean that it offers service throughout the entire block. To address this concern, the FCC recently launched a "broadband mapping" initiative to obtain more granular data about the locations where broadband is and is not offered. *See* Establishing the Digital Opportunity Data Collection; Modernizing the FCC Form 477 Data Program, 85 Fed. Reg. 50,911 (Aug. 18, 2020).

offer at least 25/3 Mbps service.[33] The number rises to 83% of the population when the speed threshold is lowered to 10/1 Mbps, which, while now substandard, is still sufficient to stream two different Netflix shows simultaneously in high definition.[34]

Advocates claiming that cable broadband is a monopoly tend to obscure the extent of competition by gerrymandering the definition of "broadband" to exclude any service that does not meet some arbitrarily defined speed benchmark (*e.g.*, 100 Mbps or 1 Gbps).[35] But such abstract definitions are economically meaningless if divorced from the facts of what consumers actually want and need. It makes no more sense to pick an aggressive speed threshold as the *sine qua non* of "broadband" than it does to define a "car" by the ability to hit sixty miles per hour in under six seconds. Consumers do not buy broadband services on the basis of arbitrary metrics; they buy the available service that meets their needs and offers them the best value for the money. So a lower-speed service (*e.g.*, 25 Mbps) can impose competitive discipline on a higher-speed service (*e.g.*, 100 Mbps) in the same way that a car model with slower but still adequate acceleration imposes competitive discipline on a similar but more expensive model with faster acceleration. And that is true whether or not all or even most consumers view the two services as close substitutes. Because "competition takes place at the margin," a lower-speed service can constrain prices for a somewhat faster-speed service even if a significant minority of consumers view the former as a good-enough substitute for the latter.[36]

Recognizing these competitive realities, some regulatory advocates avoid "monopoly" rhetoric and contend instead that fixed broadband in the U.S. is a "duopoly," consisting in each geographic market of one cable company and one telco. That description is less implausible than the "monopoly" label, but it too can be misleading. As an initial matter, it is plainly overbroad: many metropolitan areas feature competition from fixed providers in addition to the local telephone and cable companies, such as RCN

33. Specifically, as of June 2019, 69.59% of Americans lived in census blocks in which at least two terrestrial (*i.e.*, non-satellite) fixed (*i.e.*, non-mobile) providers offered speeds of at least 25/3 Mbps. *See Fixed Broadband Deployment – Area Summary*, FCC, https://broadbandmap.fcc.gov/#/area-summary (last visited Sept. 3, 2020) [https://perma.cc/9CJL-CFTD] (data from June 2019) (in Application Settings, uncheck the box labeled "Satellite"). Satellite-based services are generally not considered close substitutes for terrestrial fixed broadband because, given the finite speed of light, they are subject to significant latency, making real-time applications difficult.

34. *See Internet Connection Speed Recommendations*, NETFLIX, https://help.netflix.com/en/node/306 (last visited Sept. 20, 2020) [https://perma.cc/EGR9-47A2] ("5.0 Megabits per second . . . [r]ecommended for HD quality").

35. *See, e.g.*, Gabrielle Daley, *The Monopolies That No One Is Talking About*, PUB. KNOWLEDGE (Sept. 1, 2017), https://www.publicknowledge.org/blog/the-monopolies-that-no-one-is-talking-about/ [https://perma.cc/TUP7-JMBW] ("In 2015 the FCC redefined broadband internet" to exclude services below 25/3 Mbps, and "this classification reflects that DSL is effectively no longer in the running, and consumers have limited choices for broadband.").

36. Jerry Hausman & J. Gregory Sidak, *Telecommunications Regulation: Current Approaches with the End in Sight*, *in* ECONOMIC REGULATION AND ITS REFORM: WHAT HAVE WE LEARNED? 345, 400 (Nancy L. Rose ed. 2014).

and Google Fiber.[37] But even in areas without a third fixed competitor, "duopoly" rhetoric obscures more than it edifies, for two reasons.

First, the unusual cost structure of the broadband industry makes it more competitive than most other industries with similar levels of concentration. The "duopoly" label is typically invoked to describe classic market settings—such as two gas stations on opposite sides of a rural intersection—where prices stabilize high above competitive levels. Even in areas with only two fixed-line providers, the broadband market is much more competitive than that. In part because broadband ISPs and gas stations, like other classic retail businesses, differ in cost characteristics.[38] Gas stations have high marginal costs compared to their fixed costs; they must pay a substantial amount at wholesale for every unit of gasoline that they sell to consumers at a retail markup. For each sale that a gas station loses to its lone competitor across the highway, it saves a high percentage of the forgone retail revenues in the form of avoided costs. In contrast, broadband ISPs have small marginal costs compared to their fixed costs. Once they have made the large capital investments needed to deploy transmission lines throughout the residential neighborhoods within their geographic footprints, the marginal recurring costs of serving any particular household within those neighborhoods are very low by comparison.[39]

As we and others have pointed out, that cost structure typically results in significant price competition even in duopoly broadband markets.[40] The reason is intuitive: suppose that two broadband ISPs have deployed similar networks in the same residential neighborhood, each sufficient to serve the full demand within that neighborhood. When one broadband provider loses a household to the other, it loses all revenues associated with that household but

37. As of June 2019, more than 25% of Americans lived in census blocks with three or more terrestrial fixed broadband providers offering speeds of 25 Mbps or more, and 37.49% lived in census blocks with three or more such providers offering speeds of 10 Mbps or more. *See Fixed Broadband Deployment – Area Summary*, *supra* note 34. All of these figures, of course, exclude mobile broadband services. *Id.*

38. *See, e.g.*, Shelanski, *supra* note 14, at 89–93.

39. *See* Nuechterlein & Weiser, *supra* note 15, at 8–9.

40. *See* Shelanski, *supra* note 14, at 89–93; Nuechterlein & Weiser, *supra* note 15, at 220–21; Business Data Services in an Internet Protocol Environment, *Report and Order*, 32 FCC Rcd. 3459, para. 120 (2017) ("[T]he largest benefits from competition come from the presence of a second provider, with added benefits of additional providers falling thereafter, in part because, consistent with other industries with large sunk costs, the impact of a second provider is likely to be particularly profound in the case of wireline network providers.") (footnote omitted), *aff'd*, Citizens Telecomms. Co. of Minn., LLC v. FCC, 901 F.3d 991 (8th Cir. 2018); Timothy J. Tardiff, *Changes in Industry Structure and Technological Convergence: Implications for Competition Policy and Regulation in Telecommunications*, 4 INT'L ECON. & ECON. POL'Y 109 (2007); Dennis L. Weisman, *When Can Regulation Defer to Competition for Constraining Market Power?: Complements and Critical Elasticities*, 2 J. COMPETITION L. & ECON. 101, 102 (2006) ("[P]rice increases that produce even small reductions in demand can generate large losses in contribution to joint and common costs because the firm's revenues decline much more than the costs it can avoid. It is in this manner that high margins can serve to discipline the [de]regulated firm's pricing behavior."); *see also* Richard J. Gilbert, *Mobility Barriers and the Value of Incumbency*, *in* 1 HANDBOOK OF INDUSTRIAL ORGANIZATION 475, 520 (Richard Schmalensee & Robert Willig eds. 1989) ("[S]unk costs are likely to contribute to exit barriers.").

saves very little in the form of avoided costs. That economic reality gives each provider unusually strong incentives to offer substantial discounts in order to win and retain as many households as possible within the neighborhood, resulting in reasonably competitive equilibrium prices.[41]

None of this is to say, of course, that two-provider broadband markets are always just as competitive as three-provider broadband markets. Our point instead is that two-provider broadband markets are substantially more competitive than either one-provider broadband markets or other types of two-provider markets with higher marginal costs and lower fixed costs. That fact necessarily reduces the potential benefits of regulatory intervention. Again, whereas price regulation is very likely to bring rates closer to competitive levels in stable monopolistic markets, it is less likely to have that effect—or to have it to the same degree—in markets characterized by even imperfect levels of competition.

The other reason that two-provider broadband markets are less competitively stable than the gasoline market at our hypothetical rural intersection is that the odds of technological disruption and thus new entry are higher. The ascendance of mobile over landline telephony in the early 21st century provides an instructive analogy. As recently as ten years ago, the FCC still argued with a straight face that landline telephone companies dominated some well-defined market for ordinary voice services, despite inroads made by mobile and VoIP competitors.[42] No one could credibly make that claim today, now that the overwhelming majority of Americans rely mainly on their cellphones for voice service and most households no longer even have operational landlines.[43]

Although it is too early to make confident predictions, we may see a similar paradigm shift for broadband within the next five to ten years. Today, mobile and fixed-line broadband are partial but imperfect substitutes. By definition, fixed-line services are not mobile, and consumers place a high premium on mobility. At the same time, mobile broadband is more costly than fixed-line broadband for the most bandwidth-intensive applications, such as streaming and videoconferencing. Although 4G LTE networks easily handle those applications in the absence of congestion, mobile users must share the necessary spectrum in any given cell, and mobile plans are therefore more likely to feature usage-based pricing arrangements that constrain a typical user's consumption habits. These key differences—the "mobility gap" for

41. In economic terms, the Cournot (less competitive) model of duopolistic behavior is more likely to characterize decisions about whether to build networks in the first place, whereas the Bertrand (more competitive) model is likely to describe competitive conditions once those networks are up and running. *See* Shelanski, *supra* note 14, at 90–91 (discussing David M. Kreps & José A. Scheinkman, *Quantity Precommitment and Bertrand Competition Yield Cournot Outcomes*, 14 BELL J. ECON. 326 (1983)).

42. Petition of Qwest Corp. for Forbearance Pursuant to 47 U.S.C. § 160(c) in the Phx., Ariz. Metro. Statistical Area, *Memorandum Opinion and Order*, 25 FCC Rcd. 8622, paras. 55–58 (2010), *aff'd*, Qwest Corp. v. FCC, 689 F.3d 1214 (10th Cir. 2012).

43. *See* Felix Richter, *Landline Phones Are a Dying Breed*, STATISTA (June 15, 2020), https://www.statista.com/chart/2072/landline-phones-in-the-united-states/ [https://perma.cc/AY3F-428H].

fixed-line services and the "pricing gap" for mobile services—are the main reason why many consumers still view mobile and fixed-line broadband more as complements than as close substitutes.[44]

The line between these two services may blur however, with the rise of 5G technology. Compared to prior-generation networks, 5G networks consist of much smaller and more numerous wireless cells, connected by dense webs of fiber backhaul lines.[45] Shrinking any wireless network's cells reduces the number of users who must share spectrum in any given cell, thereby lessening the need to ration spectrum through usage-based pricing. If and when 5G network architecture enables mobile providers to close this "pricing gap" with fixed-line services, fixed-line providers may respond by accelerating the widespread deployment of wireless nodes within their own networks to close their own "mobility gap" with wireless providers.[46] That competitive dynamic would make fixed-line and mobile services closer substitutes than they are now.[47] At that point, many markets that have two competing providers today could have more than twice that number: the two legacy "fixed-line" networks plus multiple legacy "mobile" networks.

In sum, the U.S. broadband marketplace in most areas is significantly competitive today and may be poised for disruptive competitive entry within the foreseeable future. That conclusion has major implications for today's debates about whether this industry, which has been lightly regulated since its inception, should now be subject to dramatically increased levels of intervention.

---

44. As the FCC summarized this point in early 2018, "[M]obile broadband is not a full substitute for fixed broadband connections" because "fixed and mobile Internet access have different characteristics and capabilities, for example, typically trading off speed and data caps limits against mobility," but "increasing numbers of Internet access subscribers are relying on mobile services only," and "[w]ith the advent of 5G technologies promising sharply increased mobile speeds in the near future, the pressure mobile exerts in the broadband market place will become even more significant." Restoring Internet Freedom, *Declaratory Ruling, Report and Order, and Order*, 33 FCC Rcd. 311, paras. 9, 130 (2018) [hereinafter *RIF Order*], *aff'd in part and vacated in part*, Mozilla Corp. v. FCC, 940 F.3d 1 (D.C. Cir. 2019).

45. *See* Linda Hardesty, *Traditional Mobile Backhaul Won't Suffice for 5G*, FIERCEWIRELESS (Apr. 7, 2020), https://www.fiercewireless.com/5g/traditional-mobile-backhaul-won-t-suffice-for-5g [https://perma.cc/Y4QY-6D63].

46. *See* Mike Dano, *An Inside Look at Cable's MVNO Business Model*, LIGHTREADING (July 22, 2019), https://www.lightreading.com/cable/cable-wi-fi/an-inside-look-at-cables-mvno-business-model/d/d-id/752938 [https://perma.cc/5PW5-NN8W] ("Comcast and Charter have positioned WiFi as a cornerstone of their mobile strategy. And based on new figures from network-monitoring company Tutela, their efforts so far appear to be bearing fruit. Tutela found that Comcast and Charter are moving substantial amounts of customer data off Verizon's LTE network and onto WiFi networks, including their own hotspots."); *see also 5G Home*, VERIZON, https://www.verizon.com/5g/home/ (last visited Sept. 3, 2020) [https://perma.cc/N93F-3UH2] (advertising "5G Home Internet Service").

47. *See* Don Reisinger, *Home Broadband Providers Face an Uncertain Future in the 5G Era*, FORTUNE (Feb. 13, 2020, 4:00PM), https://fortune.com/2020/02/13/5g-impact-on-broadband/ [https://perma.cc/8T99-3XAS]. Again, because competition occurs at the margin, mobile services will likely impose substantial competitive discipline on fixed-line services (and vice versa) even if only a subset of consumers view them as close substitutes. *See* Hausman & Sidak, *supra* note 37, at 400.

III. ASSESSING THE COSTS AND BENEFITS OF CURRENT PROPOSALS FOR BROADBAND REGULATION

As we have explained, the benefits of economic regulation are likely to be lowest, and the threats posed by such regulation to investment and innovation are likely to be greatest, in technologically dynamic industries subject to some competition today and a prospect of additional entry tomorrow. Broadband is such an industry, so cost-benefit analysis counsels against most forms of economic regulation. U.S. policymakers have generally adhered to that proposition for the past two decades and thus, with one arguable exception, have maintained a regime of light-touch regulatory oversight, as summarized in Section III.A below. Section III.B brings a cost-benefit analysis to bear on four distinct but overlapping types of proposals for ratcheting up the level of broadband regulation—facilities sharing, price regulation, interconnection obligations, and open-ended content nondiscrimination rules. Proposals in the fourth category, which often go by the "net neutrality" label, occupy an outsized share of attention in policy debates, and our discussion of them is accordingly outsized too. Finally, we turn in Section III.C to the special costs presented by state-level economic regulation of any kind.

A. A Brief History of the U.S. Approach to Broadband Regulation

Debates about economic regulation of consumer broadband services are as old as those services themselves, which began to take root in the late 1990s. At that time, cable modem services offered by local cable franchisees accounted for the great majority of U.S. broadband Internet connections, yet they were completely free of economic regulation.[48] The *2000 NOI* sought public comment on that policy and, in particular, on so-called "open access" proposals, which would have required cable broadband providers to lease portions of their physical networks to third-party ISPs such as AOL and Earthlink.[49] Two years later, the FCC rejected those proposals on the ground (among others) that they would undermine incentives for continued broadband investment by cable companies and their facilities-based competitors.[50] That decision also reflected a degree of technological pragmatism: there was never an engineering consensus on how cable companies could feasibly "unbundle" the broadband transmission

48. *See* Nuechterlein & Weiser, *supra* note 15, at 192–96; *see also* Stephen Labaton, *Fight for Internet Access Creates Unusual Alliances*, N.Y. TIMES, Aug. 13, 1999, at A1.

49. *2000 FCC NOI*, *supra* note 5.

50. Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, *Declaratory Ruling and Notice of Proposed Rulemaking*, 17 FCC Rcd. 4798, paras. 4–5 (2002), *aff'd*, Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967 (2005).

components of their networks, which were heterogeneous and not designed with such sharing obligations in mind.[51]

Ironically, legacy FCC rules at the time did impose the type of unbundling obligations on telephone companies that the FCC declined to impose on cable companies, even though the former lagged well behind the latter in share of broadband connections. In particular, wireline telephone companies were subject to the *Computer Inquiry* rules, which the FCC originally adopted in the 1970s and 80s before the advent of cable broadband, when the telephone system was the only means of access to online data services.[52] These legacy rules did not regulate the *retail* broadband Internet access service sold by telephone companies to consumers, and those services were mostly unregulated at both the state and federal level. But the rules did require any telco offering such a service to "unbundle" the transmission component (usually a DSL line), tariff it as a common carrier service, and offer it for sale on a wholesale basis to any third-party ISP.[53] In 2005, the FCC eliminated that requirement as it applied to these residential broadband services, citing the investment disincentives of such regulation and noting the paradox that those rules never applied to cable companies, with their larger

51. That lack of consensus manifested itself when the FTC sought to implement an "open access" merger condition it had imposed on AOL's acquisition of Time Warner Cable in 2000. Christopher Yoo wrote at the time:

> Contrary to the original expectations of the FTC, the unaffiliated ISPs that have obtained access to AOL-Time Warner's cable modem systems under the FTC's merger clearance order have not placed their own packet network and backbone access facilities within AOL-Time Warner's headends. Instead, traffic bound for these unaffiliated ISPs exits the headend via AOL-Time Warner's backbone and is handed off to the unaffiliated ISP at some external location. It is hard to see how consumers benefit from such arrangements, given that they necessarily use the same equipment and thus provide the same speed, services, and access to content regardless of the identity of their nominal ISP. The fact that these unaffiliated ISPs have found it more economical to share AOL Time Warner's existing ISP facilities rather than build their own strongly suggests that integrating ISP and last-mile operations does in fact yield real efficiencies.

Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debate*, 3 J. TELECOMM. & HIGH TECH. L. 23, 55–56 (2004) (footnote omitted).

52. *See* Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities, *Report and Order and Notice of Proposed Rulemaking*, 20 FCC Rcd. 14853, paras. 21–31 (2005) [hereinafter *Wireline Broadband Order*], *aff'd*, Time Warner Telecom, Inc. v. FCC, 507 F.3d 205 (3d Cir. 2007).

53. *See id.*; *see also* Nuechterlein & Weiser, *supra* note 15, at 69–71. For a time, the FCC separately required incumbent local exchange carriers under the 1996 Act to lease the "high frequency portion" of last-mile copper lines (*i.e.*, the frequency range used for data rather than voice transmissions) to telecommunications carriers associated with third-party ISPs. The FCC moved to eliminate such "line-sharing" obligations in 2003 after the D.C. Circuit expressed skepticism that it made sense to impose them on telephone companies but not the market-leading cable companies.

broadband shares.[54] Two years later, the FCC extended the same deregulatory approach to the emerging class of mobile broadband networks.[55]

Subsequent years have seen only modest upticks in the degree of regulation imposed on broadband providers. Of course, in determining how "heavy" or "light" any broadband regulatory scheme may have been, the relevant question is not how many lines of text appeared in the Code of Federal Regulations. Instead, the question is whether a given regulatory scheme actually altered, or threatened to alter, the conduct that ISPs otherwise would have undertaken. Viewed from that perspective, the FCC has, for the most part, regulated broadband lightly. It has never subjected broadband ISPs to retail rate caps or any of the other hallmarks of traditional telephony regulation. Nor, since the sunset of the *Computer Inquiry* rules fifteen years ago, has it required any ISP to lease its broadband assets to competitors. True, the FCC has periodically subjected ISPs to various forms of net neutrality oversight. But apart from the brief "Title II" interlude discussed below, it has done so with a light touch and has rarely disrupted the actual business plans of ISPs.

In broad strokes, then, U.S. broadband regulation has been exceptionally light since the turn of the millennium. And as explained in Section II, that light touch approach has coincided with extraordinary investments in broadband infrastructure and a proliferation of increasingly high-speed fixed-line and mobile broadband services. That history is important because, despite these market successes, there are today rising calls for substantially ratcheting up the level of regulation—either by picking up where the Title II regime left off in 2016 and following through on its potential for regulatory creep (as discussed below) or, more radically, by imposing full-blown price controls or facilities-sharing obligations on broadband providers. In the discussion that follows, we weigh the ostensible benefits of such proposals against the potential costs.

B. The Costs and Benefits of Proposals for New Broadband Regulation

1. Facilities-Sharing Obligations

For many years, advocates of greater regulation have claimed that the U.S. has "fallen behind" other major industrialized nations in broadband performance metrics, such as throughput speeds and quality-adjusted price. These critics attribute that perceived performance gap to the less regulated nature of U.S. broadband markets and contend that it can be closed by

54. *See Wireline Broadband Order*, *supra* note 53, ¶¶ 44, 51–52. The FCC nonetheless permitted carriers, if they so chose, to continue tariffing a bare DSL transmission service, unbundled from internet access. A number of small rural telephone companies had requested that option so that they could continue availing themselves of certain benefits under the legacy regulatory regimes applicable to such companies. *Id.* ¶¶ 89–95, 48 n.269.

55. *See* Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks*, Declaratory Ruling*, 22 FCC Rcd. 5901 (2007).

importing the facilities-sharing (or "structural separation") regime found in (for example) the United Kingdom or Australia, where the dominant network is formally separated from any retail operations and must lease capacity on regulated wholesale terms to third-party ISPs. That approach, these critics say, is the key to greater competition and, with it, faster speeds and lower prices.[56]

As a threshold matter, these proposals rest on the empirical premise that the U.S. actually is, in some relevant sense, "behind" its international peers in terms of broadband speeds and quality-adjusted prices. But that premise is fiercely contested, in part because many confounding variables complicate true apples-to-apples comparisons.[57] For example, network costs per consumer and thus retail prices depend in large part on economies of density, and the countries subject to these comparisons have vastly different population densities—the U.S. averages eighty-seven people per square mile, whereas the U.K. averages 725 and South Korea averages 1,338.[58] And some international comparisons, including the FCC's, have found that U.S. fixed-line broadband metrics are in fact superior to those of most peer nations once appropriate adjustments are taken into account.[59] The peer nations with

56. For example, writing in *The New Yorker* in 2016, NYU Professor Chris Sprigman argued that the recently imposed Title II net neutrality rules were insufficient to address the broadband's putative "monopoly" problem and that the FCC should "mandate what telecom geeks refer to as 'local-loop unbundling.'" Sprigman, *supra* note 27. "If that happened, new companies would arise to connect to the cable giants' networks and vie to provide broadband access. That new competition would push down prices, improve service, spark innovation, and also ease the concerns about discrimination that provoked the F.C.C.'s net-neutrality mandate in the first place." *Id.*; *see also* Ian Bogost, *Net Neutrality Was Never Enough*, THE ATLANTIC (Dec. 15, 2017), https://www.theatlantic.com/technology/archive/2017/12/net-neutrality-was-never-enough/548549/ [https://perma.cc/9ZV6-YJUU]; Peter Bright, *We Don't Need Net Neutrality; We Need Competition*, ARS TECHNICA (June 26, 2014), https://arstechnica.com/tech-policy/2014/06/we-dont-need-net-neutrality-we-need-competition/ [https://perma.cc/3DPX-HGWV].

57. *Compare*, *e.g.*, Becky Chao & Claire Park, *The Cost of Connectivity*, NEW AM. 32–38 (2020), https://d1y8sb8igg2f8e.cloudfront.net/documents/The_Cost_of_Connectivity_2020__XatkXnf.pdf [https://perma.cc/M3NY-7MAV], *with* Michael J. Santorelli & Alexander Karras, *The Value of Context and Rigor: A Review of OTI's Cost of Connectivity 2020 Report*, ADVANCED COMMC'NS L. & POL'Y INST. AT N.Y. LAW SCH. 6–7, 12–13 (July, 2020), http://comms.nyls.edu/ACLP/ACLP-Review-of-OTI-COC-2020-Report-July-2020.pdf [https://perma.cc/3Y3J-9WAX].

58. *List of Countries and Dependencies by Population Density*, WIKIPEDIA, https://en.wikipedia.org/wiki/List_of_countries_and_dependencies_by_population_density (last visited Sept. 20, 2020) [https://perma.cc/4Q5U-4HPC].

59. *See* Int'l Comparison Requirements Pursuant to the Broadband Data Improvement Act, *Sixth Report*, 33 FCC Rcd. 978, paras. 11, 14 (2018) (finding (1) that U.S. fixed-line broadband "speeds and international rank have been on a rising trend since 2012" and have "risen to 10th fastest of 28 countries in 2016" and (2) that after "adjust[ing] for cost, demographic, and quality differences across the countries . . . the United States ranks 7th out of the 29 countries" in broadband pricing).

reportedly inferior network performance include the U.K. and Australia, two countries with oft-cited facilities-sharing regimes.[60]

It is beyond the scope of our paper to resolve these empirical disputes. Our main point here is that *even if* the U.S. lagged peer nations in broadband metrics, it could not possibly narrow that gap by subjecting broadband ISPs to a new battery of facilities-sharing obligations, with all the attendant operational costs, business risks, and regulatory uncertainty. To the contrary, such obligations would undermine incentives for new broadband investment and harm the very consumers they are meant to benefit.

To begin with, the potential benefits of facilities-sharing obligations are both limited and generally confined to monopoly markets without facilities-based competition. As we have discussed, that description does not generally fit U.S. broadband markets, but it does fit broadband markets in some OECD countries, which are typically dominated by one facilities-based fixed broadband provider (the legacy telephone system). Regulators in some of those OECD jurisdictions have indeed promoted a form of resale competition by entitling non-facilities-based ISPs to lease the incumbent telco's network facilities at regulated wholesale rates. These network sharing regimes, however, are a pale substitute for facilities-based competition, and they can make sense (if at all) only when policymakers see no real prospect of such competition.

Although network-sharing regimes do create some competition at the retail level, that competition is limited because the competitors by definition all share the same underlying network assets. For example, although the incumbent and the competitors using its network do compete on the basis of retail prices, the competitors' prices are largely a function of whatever wholesale rate regulators prescribe. Instead of capping retail rates, regulators cap wholesale rates, which are then passed through to consumers in the form of higher or lower retail rates. Ultimately, retail prices are kept in check not so much by competitive dynamics as by an indirect form of rate regulation. The non-price dimensions of competition are similarly limited by the deployment and engineering decisions the incumbent has made. It is thus illogical to suppose that network-sharing obligations would usher in a new era of ever-faster speeds and lower quality-adjusted prices. And on the other side of the cost-benefit ledger, such obligations impose major costs, as discussed below, which cannot be justified in the absence of durable monopoly power. In Justice Stephen Breyer's words, "[r]egulatory rules that go too far, expanding the definition of what must be shared beyond that which

60. *See id.* at app.B, tbl.2; *see also* Robert D. Atkinson & Doug Brake, *How Broadband Populists Are Pushing for Government-Run Internet One Step at a Time*, INFO. TECH. & INNOVATION FOUND. 8 (Jan. 2017), http://www2.itif.org/2017-broadband-populism.pdf [https://perma.cc/8EEX-LLPX] (noting that "Australia is actually pursuing the model espoused by many broadband populists—full structural separation, with government ownership of the underlying infrastructure and retail competition on top" and that, "on average, Australia continues to have relatively high prices and low speeds compared with other countries").

is essential to that which merely proves advantageous to a single competitor, risk costs that . . . may make the game not worth the candle."[61]

A page of history here is worth a pound of logic because the U.S. has already had a largely unsuccessful experience with this very type of regime—the FCC's "local competition" rules implementing the Telecommunications Act of 1996. The purpose of those rules may seem quaint now. In 1996, policymakers focused mainly on boosting competition among local providers of landline telephone service, which they viewed as an entrenched monopoly.[62] As its tool of choice for opening those markets, the FCC required incumbents to lease to any new entrant the piece parts of their telephone networks, known as "unbundled network elements" or "UNEs." The big questions of the day included the regulated terms by which a new entrant (*e.g.*, a "long distance" carrier such as AT&T Corp. or MCI) could lease copper loops and circuit-switching capacity from incumbent local telcos (*e.g.*, Bell Atlantic and Southwestern Bell). [63] For many years, the FCC ordered incumbents to lease to an aspiring rival *all* of the network elements it needed to provide circuit-switched telephony, including shared access to the circuit switch itself—an arrangement known as "UNE-P" (for "unbundled network element platform").[64] In a series of decisions in the early-to-mid 2000s, the D.C. Circuit finally invalidated that maximally regulatory approach on the ground that it produced no more than "completely synthetic competition" and came "at a cost, including disincentives to research and development by both [incumbents] and [entrants] and the tangled management inherent in shared use of a common resource."[65]

Of course, sharing obligations require regulators not only to identify which facilities must be leased to rivals, but also to set the rates that incumbents may charge for leasing them. To that end, the FCC directed state public utility commissions to base wholesale rates for all network elements on an arcane cost methodology known as "total element long-run incremental cost," or TELRIC.[66] A generation of lawyers and economists got rich arguing about how to implement that methodology, which required modeling how a hypothetical efficient firm would build a new wireline telephone network, taking as given only the locations of the "wire centers" the incumbent telephone monopolist chose many decades previously for the routing of circuit-switched voice calls.[67] One of the many conundrums in applying this methodology was that no efficient firm at the turn of the millennium would have built such a network in the first place because circuit-switched landline telephony was a technology in decline.

---

61. AT&T Corp. v. Iowa Utils. Bd., 525 U.S. 366, 430 (1999) (Breyer, J., concurring in relevant part and dissenting on other grounds).

62. *See* Nuechterlein & Weiser, *supra* note 15, at 51–53.

63. *See id.* at 58–60.

64. *See id.* at 62–66.

65. U.S. Telecomm. Ass'n v. FCC (USTA I), 290 F.3d 415, 424, 429 (D.C. Cir. 2002); *see also* U.S. Telecom Ass'n v. FCC, 359 F.3d 554 (D.C. Cir. 2004); Covad Commc'ns Co. v. FCC, 450 F.3d 528 (D.C. Cir. 2006).

66. 47 C.F.R. § 51.505.

67. *Id.*

In the end, the main entrants that had based their business plans on leasing last-mile telco facilities collapsed when consumers and investors saw that the future of communications lay elsewhere.[68] Meanwhile, the competitors that built new cellular and broadband networks, which bypassed last-mile telco infrastructure completely, were the ones that brought real competition and innovation to U.S. telecommunications markets, without reliance on the FCC's elaborate regulatory apparatus. The great irony of this era was that, by allowing those services to grow with minimal regulation, policymakers refuted their own premise that highly disruptive regulation was needed to bring competition to legacy wireline technologies.

If "[t]hose who cannot remember the past are condemned to repeat it,"[69] the rise and fall of UNE-based local exchange competition serves as a cautionary tale for broadband policymakers today, as they consider arguments that broadband is inadequately competitive and that the solution lies in complex facilities-sharing rules. Indeed, such rules would be even less appropriate for the broadband marketplace of today than for the telephone market of 1996. Whereas local exchange markets in 1996 were true (if declining) monopolies, today's fixed broadband market already exhibits significant facilities-based competition, as we have discussed. And today's fixed broadband providers also face a realistic near-term prospect of additional disruptive competition, as mobile providers deploy 5G networks. Those considerations reduce the need for, and magnify the risks of, elective regulatory surgery in the form of rules designed to promote *non*-facilities-based competition. Again, the benefits of such "completely synthetic competition" are meager, particularly when a market already features facilities-based competition, and they come "at a cost, including disincentives to research and development by both [incumbents] and [entrants] and the tangled management inherent in shared use of a common resource."[70]

2. Rate Regulation

As discussed in Section III.B.4 below, the FCC has always expressed opposition to broadband rate regulation, even during the relatively interventionist Title II era of 2015-2016. But there have been increasing calls to impose such regulation anyway.

For example, as a presidential candidate in 2019, Senator Bernie Sanders vowed to "regulate [broadband ISPs] like a utility" and direct the FCC to "review prices and regulate rates where necessary."[71] In 2018, Senator Chuck Schumer likewise suggested that broadband ISPs are "essential . . . [u]tilities" and that policymakers should no longer "let them

68. *See* Nuechterlein & Weiser, *supra* note 15, at 53, 66–67.

69. 1 GEORGE SANTAYANA, THE LIFE OF REASON 284 (1905).

70. USTA I, 290 F.3d at 424, 429 (citing *Iowa Utils. Bd.*, 525 U.S. at 428–29).

71. Jon Brodkin, *Bernie Sanders Vows to Break Up Huge ISPs and Regulate Broadband Prices*, ARS TECHNICA (Dec. 7, 2019), https://arstechnica.com/tech-policy/2019/12/bernie-sanders-vows-to-break-up-huge-isps-and-regulate-broadband-prices/ [https://perma.cc/3RMG-C5TR].

charge whatever they want."[72] The *Los Angeles Times* business columnist writes that "[s]ervice providers should have to justify rate increases just like other utilities. If higher prices are warranted by legitimate operating costs, so be it. If not, go pound sand. . . . Give state public utilities commissions the power to oversee internet pricing."[73] And some states are proposing to do precisely that by requiring ISPs to offer "affordable" broadband service in a variety of circumstances.[74]

Here, it is important to distinguish between means and ends. Few dispute that all Americans should have access to high-quality broadband at affordable rates. The question is whether to meet that objective by expanding public subsidy programs or instead, by capping ISP retail rates, analogous to price controls imposed by the FCC and states on telephone monopolists in the 20th century. The former approach is appropriate and indeed critical, as we discuss in Section IV below. The latter approach, however, would be exceptionally counterproductive.

By limiting returns on a regulated firm's capital investments, price regulation necessarily reduces that firm's incentives to make such investments. While it might be fashionable to scoff at that proposition, the link between a firm's expected returns and investment decisions is hard to dispute. In durable monopoly markets, society might well have good reasons for reducing the already minimal investment incentives of an entrenched monopolist in exchange for low, regulated prices. But the costs of price regulation are much greater, and the societal benefits much lower, where some degree of competition already disciplines prices and gives firms incentives to keep up with rivals through massive, ongoing investments.

Much like facilities-sharing rules, rate caps would also undermine prospects for competitive entry and expansion in such dynamic markets. Even

---

72. John Eggerton, *Schumer: Consumers May Need Internet Affordability Protections*, MULTICHANNEL NEWS (May 9, 2018), https://www.multichannel.com/news/schumer-consumers-may-need-internet-price-protections [https://perma.cc/86YW-KG3G]; *see also* Karl Bode, *Schumer: Broadband Is a Utility That May Require Price Caps*, DSLREPORTS (May 10, 2018), http://www.dslreports.com/shownews/Schumer-Broadband-is-a-Utility-That-May-Require-Price-Caps-141803 [https://perma.cc/2SHP-ESPH] ("During his floor argument for a Congressional Review Act resolution that would restore net neutrality, Schumer stated that he believes that broadband should be viewed as an essential utility, and that we may need to eventually explore price caps to prevent monopolies from over-charging for services thanks to limited competition.").

73. David Lazarus, *Column, It's Time to Regulate Internet Service Like Any Other Utility*, L.A. TIMES (Feb. 25, 2020), https://www.latimes.com/business/story/2020-02-25/regulating-internet-service-utility [https://perma.cc/H6RD-53TC]; *see also* Steve Andriole, *It's Time for an Internet-for-All Public Utility (Before Corona Crashes It)*, FORBES (Mar. 30, 2020), https://www.forbes.com/sites/steveandriole/2020/03/30/its-time-for-an-internet-for-all-public-utility-before-corona-crashes-it/#141b5dc9af95 [https://perma.cc/UN5Y-V97G] ("As a public utility, service providers should be required to offer affordable high-speed broadband to all Americans[.] Sure, this is controversial, but it is really?").

74. *See, e.g.*, S. 1058, sec. 3, 2019-20 Leg., Reg. Sess. (Cal. introduced Feb. 18, 2020) (proposing, on a permanent basis, to "direct every internet service provider . . . to file emergency operations plans" that would include "an affordable class of broadband internet service" that the ISP "shall offer as emergency relief within its service footprint for any individual displaced by a disaster or under guidance to stay at home during a state or local emergency").

if the caps apply only to "incumbent" or "dominant" providers (however defined), they would still lower the revenue expectations of any new entrant, which would have to undersell not what the incumbents would have charged, but the substantially lower rates that regulators impose. For example, capping the retail prices of fixed-line providers would inevitably chill any mobile provider's incentives to make the risky investments needed to compete head-to-head with them because those price caps would reduce the mobile provider's own expected revenues. As was the case when the FCC issued the *National Broadband Plan* ten years ago, the major challenges facing broadband policymakers today still involve creating adequate incentives for private enterprise to invest risk capital in faster and more widespread broadband networks. Price controls would undermine that objective.

These concerns, moreover, apply not only to rate regulation that is explicitly styled as such, but also to other forms of regulation that ultimately amount to rate regulation. For example, under the unbundling regimes discussed earlier, the rates charged by new entrants are largely a function of the wholesale lease rates charged by the incumbent. And because the incumbent often does not wish to lease its network assets in the first place, regulators must cap wholesale rates. Unbundling obligations can thus be conceptualized as an indirect form of retail rate regulation, but at an even greater level of complexity, given the need for regulators and market participants to manage the non-price details of compulsory asset-sharing obligations.

Finally, but no less important, the line between "price" and "non-price" regulation is thin, and regulatory obligations can amount to rate regulation even when regulators do not perceive themselves as setting rates at either the retail or wholesale level. We address that point in detail below, where we analyze proposals to require interconnection at a regulated rate of zero (Section III.B.3) and to ban "zero-rating" programs, the economic equivalent of bundled discounts (Section III.B.4).

3. Interconnection Obligations

The Internet is composed of many different IP networks, most of them privately owned, and each network must find some way to connect its users with the users on every other network, either directly or indirectly. Since the inception of the commercial Internet, the government has left the terms of these "interconnection" arrangements to market forces, in the form of

unregulated, privately negotiated peering and transit agreements.[75] The government's hands-off approach to these *Internet* interconnection arrangements has always stood in stark contrast to the FCC's pervasive regulation of interconnection on the public switched *telephone* network ("PSTN"). For decades, regulators have determined when one telephone company must physically interconnect with others, on what terms, and with what exchange of "intercarrier compensation."[76] As every telecom lawyer knows, the resulting regulatory disputes have been nearly unrivaled in their byzantine complexity for four decades.[77]

Over the past dozen years, Netflix and other senders of high-bandwidth, one-way Internet traffic ("content networks") have urged the FCC to take a page from the PSTN rulebook and regulate Internet interconnection arrangements for the first time.[78] In particular, these advocates seek "bill and keep" rules that would entitle content networks to demand direct interconnection with residential ("eyeball") ISP networks without any exchange of compensation. They begin with the premise that any residential ISP, however small, enjoys a "terminating access monopoly" that enables it to extract supracompetitive rates from interconnecting content providers. And they conclude that the optimal solution is not a regulated positive rate, but a universal price of zero for interconnection.[79] Under that approach, any residential ISP would have to recover from its retail customers, rather than from interconnecting networks, all of the incremental costs it incurs for handling the incremental traffic loads sent by those networks.

---

75. "Peering" and "transit" describe forms of *direct* and *indirect* interconnection, respectively, between IP networks. Two IP networks enter into a peering arrangement if they interconnect *directly* and if each IP network provides the other with access *only to its own customers* (including transit customers that serve end users of their own) rather than to the entire internet. If no peering agreement enables Network X to reach a customer on Network Y, it will typically buy a transit service from intermediary Network Z to reach that customer; Z essentially acts as X's agent in ensuring *indirect* connectivity between X and Y. *See generally* Michael Kende, *The Digital Handshake: Connecting Internet Backbones* 5–7 (Off. of Plans & Pol'y, FCC, Working Paper No. 32, 2000), https://www.fcc.gov/reports-research/working-papers/digital-handshake-connecting-internet-backbones [https://perma.cc/Q2X9-9UZA]. Transit arrangements always involve the payment of compensation; peering arrangements may or may not. Over time, interconnection agreements among IP networks have grown more complex and now involve more types of direct interconnection than before, but the basic economic relationships remain similar to those found in traditional peering and transit arrangements. *See generally* Peyman Faratin et al., *The Growing Complexity of Internet Interconnection*, 72 COMM. & STRATEGIES 51 (2008); Stanley M. Besen & Mark A. Israel, *The Evolution of Internet Interconnection from Hierarchy to "Mesh": Implications for Government Regulation*, 25 INFO. ECON. & POL'Y 235 (2013).

76. *See* Nuechterlein & Weiser, *supra* note 15, at 243–93.

77. *Id.*

78. *See, e.g.*, Reply Comments of Incompas at Ex. B, Restoring Internet Freedom, WC Docket No. 17-108 (Aug. 30, 2017) (economic analysis of David S. Evans), https://www.incompas.org/files/INCOMPAS%20RIF%20Reply%20Comments-30Aug%20FINAL.pdf [https://perma.cc/LUG7-S6Z4]. For a response to Dr. Evans' advocacy, see Attachment to Letter of AT&T Services Inc., *Restoring Internet Freedom*, WC Docket No. 17-108 (Oct. 31, 2017) (economic analysis of Mark Israel and Bryan Keating), https://ecfsapi.fcc.gov/file/1031716115908/Israel-Keating%20FINAL%20103117.pdf.

79. *See* Nuechterlein & Weiser, *supra* note 15, at 287–90.

The FCC has consistently rejected such proposals, including in the 2015 *Title II Order*, which—as discussed below—set the high-water mark for regulatory intervention. The FCC found there that "the best approach [to Internet interconnection disputes] is to watch, learn, and act as required, but not intervene now, especially not with prescriptive rules."[80] That is the correct policy call, for reasons that we have elsewhere explained in depth.[81] Although the details are complex and beyond the scope of this paper, a few points warrant emphasis.

First, a content network has competitive alternatives to direct interconnection and, indeed, does not need to deal with an ISP at all to ensure the delivery of its traffic to that ISP's customers. Instead, it can purchase transit or similar services from one or more third-party networks that do interconnect with the ISP's network, and the market for such services appears highly competitive.[82] As long as it remains so, the availability of transit alternatives will substantially constrain the fees that ISPs can charge for direct interconnection. *Second*, for the same reason, it is meaningless to describe an ISP as a "terminating monopolist"; so long as it offers its customers access to the Internet, it will have to interconnect with many other networks, and those networks thus remain available to any content provider as indirect paths to the ISP's end users. Again, those alternative paths deprive the ISP of "bottleneck"

80. Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd. 5601, para. 31 (2015) [hereinafter *Title II Order*], *aff'd*, U.S. Telecom Ass'n v. FCC, 825 F.3d 674 (D.C. Cir. 2016).

81. *See* Nuechterlein & Weiser, *supra* note 15, at 284–90; Jonathan E. Nuechterlein & Christopher S. Yoo, *A Market-Oriented Analysis of the "Terminating Access Monopoly" Concept*, 14 COLO. TECH. L.J. 21 (2015); *see also* Besen & Israel, *supra* note 76.

82. *See* Applications of XO Holdings and Verizon Communications Inc. for Consent to Transfer Control of Licenses and Authorizations, *Memorandum Opinion and Order* 31 FCC Rcd. 12501, para. 44 n.156 (2016) ("[T]ransit prices have fallen by more than 90 percent in the last five years alone[.]"); *see also* Dan Rayburn, *North American Transit Pricing From Major Providers Down 10%*, STREAMING MEDIA (July 25, 2016), https://www.streamingmedia.com/Articles/Editorial/Featured-Articles/North-American-Transit-Pricing-From-Major-Providers-Down-10-112398.aspx [https://perma.cc/2VMU-NPMS] ("North American transit pricing, on average, is down about 10 percent, year-over-year."); William B. Norton, *What Are the Historical Transit Pricing Trends?*, DRPEERING INT'L, http://drpeering.net/FAQ/What-are-the-historical-transit-pricing-trends.php (last visited Sept. 17, 2020) [https://perma.cc/Q647-AU86] (showing double-digit annual percentage declines in transit prices).

or "monopoly" power in negotiating direct interconnection agreements.[83] *Third*, there is no evidence that the fees charged for indirect interconnection are particularly large, let alone supra-competitive, and the limited data available to the public suggest that such fees are generally small and competitively immaterial.[84]

Fourth, contrary to some advocacy for Internet interconnection regulation, the mere fact that one network pays another as part of direct interconnection agreements is not a sign of market failure; to the contrary, such payments can be highly efficient. An ISP network acts as an intermediary in an essentially double-sided market between its retail customers and content networks and may efficiently recover its costs from either side of the market or from both. Under well-established economic principles, whatever payments the ISP receives from content networks on one side of that market impose downward pressure on the retail rates that the ISP charges to consumers on the other side.[85] There is no reason to suppose that consumers would be better off or that the relevant markets would function more efficiently, if an ISP were forced to recover all of its costs from

83. The widespread availability of many indirect routes into any given ISP's network is one of several factors that distinguishes Internet interconnection from PSTN interconnection and makes efficient outcomes more likely in the absence of regulation. *See* Nuechterlein & Yoo, *supra* note 82. Significantly, it is the content network that chooses an indirect path into an ISP's network, not the ISP network (which has no control over the content network's choice of intermediary network), and content networks often "multihome" their traffic among several intermediaries simultaneously. An ISP therefore could not force content providers into a direct interconnection agreement unless it simultaneously degraded all of those alternative paths into (and out of) its network, thereby destroying the value of its service to its own retail customers. Regulatory advocacy on these issues tends to obscure that technological reality—and also to overlook the possibility that content networks themselves have created congestion in hopes of obtaining regulatory intervention. *See, e.g.*, Dan Rayburn, *Cogent Now Admits They Slowed Down Netflix's Traffic, Creating A Fast Lane & Slow Lane*, STREAMINGMEDIA (Nov. 5, 2014), https://www.streamingmediablog.com/2014/11/cogent-now-admits-slowed-netflixs-traffic-creating-fast-lane-slow-lane.html [https://perma.cc/SMC3-K6X3].

84. *See* Applications of Comcast Corp., Time Warner Cable Inc., Charter Communications, Inc., and SpinCo for Consent to Assign or Transfer Control of Licenses and Authorizations, *Opposition to Petitions to Deny and Response to Comments*, MB Docket No. 14-57, FCC, para. 44, Ex. 4 (2014) (reporting that Netflix executive thanked Comcast for finding "middle ground on our [interconnection] issues that worked well for both of us for the long term, and works great for consumers" and that Comcast "made paid peering affordable for us."); *Edited Transcript, Q2 2014 Netflix Inc Earnings Call*, REUTERS 6 (July 21, 2014), https://s22.q4cdn.com/959853165/files/doc_financials/quarterly_reports/2014/q2/NFLX-Transcript-2014-07-21.pdf [https://perma.cc/B3QS-GGYB] (Analyst question: "If . . . we don't have strong net neutrality [rules] going forward, how do investors get assurances that the business is protected, in terms of cost, perhaps interconnection costs over time?" Netflix answer: "Well on a short-term basis, I think there's great assurances in the sense that we've been able to sign these immediate interconnect deals, and still able to achieve our margin targets. . . . [F]or Netflix, content is our largest cost. It dwarfs all of the other costs[.]").

85. *See, e.g.*, ROBERT E. LITAN & HAL J. SINGER, THE NEED FOR SPEED: A NEW FRAMEWORK FOR TELECOMMUNICATIONS POLICY FOR THE 21ST CENTURY 43 (2013) (addressing "see-saw principle").

consumers and none from interconnecting content networks.[86] To the contrary, allowing an ISP to recover some costs from such networks would increase efficiency and benefit consumers if it creates additional incentives for those networks to economize on the traffic loads they send into ISP networks—for example, by using more efficient forms of digital compression.

In short, as with the other forms of regulatory intervention we have discussed, creating a new set of IP interconnection rules would serve no apparent purpose and might foreclose efficient arrangements for ISP cost recovery. In addition, such rules would embroil the industry in a new generation of regulatory disputes. There would be nothing simple about imposing a bill-and-keep scheme on interconnection arrangements. Although the price (zero) is obviously straightforward, regulators would find themselves mired in obscure controversies about exactly when to mandate direct interconnection between any two networks, where on one network the other network could demand interconnection, who must pay for capacity upgrades, and so forth. These are not details that regulators are well-equipped to resolve, and as discussed, there is no need for them to do so in the first place.

4. Open-Ended ISP Conduct Rules

The term "net neutrality" describes a loose set of policy concerns that focus not on the horizontal dimension of competition among rival broadband ISPs, but on the vertical relationships between each ISP (whether it faces competition or not) and providers of complementary Internet content and applications. For example, all forms of net neutrality regulation would prohibit any mass market broadband ISP from blocking or degrading disfavored Internet traffic without a reasonable "network management" justification.[87]

Judging solely from newspaper headlines and partisan vote counts, net neutrality would appear to be one of the most divisive issues in regulatory policy today. But there is far more consensus about the underlying policy

86. *See* Nuechterlein & Yoo, *supra* note 82, at 32 n.27 ("Large volumes of incoming traffic impose costs on ISP networks. ISPs could efficiently recover those costs by charging higher retail rates to their heaviest data users or, alternatively, by charging wholesale rates to the networks that offload high volumes of unidirectional traffic. Suppose that, in the latter scenario, the interconnecting network that pays these wholesale charges is a CDN operated by a subscription streaming-video provider such as Netflix. Ultimately, the video provider will pass some or all of the charges through to its subscribers in the form of higher rates for its service, and it can vary those rates explicitly depending on each subscriber's ISP and the wholesale rates that ISP charges for interconnection. Under either scenario, the costs caused by the extra streaming video traffic will be paid by the end users that benefit from that traffic and cause it to be transmitted. There is no reason in principle why either of these cost-recovery models is inherently more efficient than the other.").

87. Net neutrality issues are related to, but distinct from, questions about Internet interconnection. Whereas interconnection issues address whether an ISP should be compelled to interconnect directly (rather than indirectly) with other networks and on what terms, net neutrality issues generally address whether and when an ISP may discriminate among packets already on its network.

questions than all the angry rhetoric would suggest and ISPs have publicly disavowed the conduct that core net neutrality rules are designed to prohibit.[88] Indeed, one might be tempted to think that, like academic politics, the politics of net neutrality is "the most vicious and bitter form of politics, because the stakes are so low."[89] That observation however, is subject to an important caveat, which we address below: open-ended "nondiscrimination" obligations for consumer broadband services, if unaccompanied by economically sensible limiting principles, can do real harm by shading into rate regulation, creating regulatory uncertainty, and ultimately deterring broadband investment and innovation.

a. Some economic context is important at the outset. Vertical relationships among firms at different levels of the value chain are ubiquitous in the modern economy, and most of them are completely unregulated.[90] Such relationships typically warrant antitrust or regulatory intervention only when one firm dominates the market at one level, potentially—though not inevitably or even usually—to the detriment of competition at other levels.[91] But advocates of net neutrality rules would not restrict those rules to circumstances where one ISP dominates a local broadband market; instead, they would apply net neutrality rules to all ISPs, irrespective of competitive conditions. As justification, they cite, among other things, the positive externalities generated by the Internet as an open and ubiquitously accessible platform for communication and innovation. Under this analysis, private actors could pursue their own rational self-interest, even in highly competitive markets, yet act in ways that threaten to fragment the Internet and reduce its positive externalities.[92]

That point is theoretically plausible and might well justify regulatory intervention if unregulated ISPs acted in ways that threaten the essential openness of the Internet. But the risk of such outcomes seems attenuated today because core net neutrality principles are now industry norms bolstered by strong consumer expectations. For example, from 2010 until 2017, the FCC's net neutrality regime included a bright-line prohibition on blocking or throttling by ISPs of disfavored Internet content without a network

88. *See, e.g.*, *ISPs Commit to an Open Internet*, NCTA, https://www.ncta.com/chart/isps-commit-an-open-internet?share_redirect=%2Ftopics#colorbox=node-3292 (last visited Dec. 5, 2020) [https://perma.cc/8TLJ-8BNZ].

89. This quote about academic politics has been attributed to Columbia political science professor Wallace Stanley Sayre and is sometimes known as "Sayre's Law."

90. *See generally* Francine Lafontaine & Margaret Slade, *Vertical Integration and Firm Boundaries: The Evidence*, 45 J. ECON. LITERATURE 629 (2007); James C. Cooper et al., *Vertical Antitrust Policy as a Problem of Inference*, 23 INT'L J. INDUS. ORG. 639 (2005).

91. *See* Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age*, 17 HARV. J.L. & TECH. 85, 107 (2003).

92. *See, e.g.*, BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES 331 (2012) (arguing that the "social value of the Internet greatly exceeds [the] market value" that would be reflected in consumers decisions even in fully competitive markets); *see also Title II Order*, *supra* note 81, ¶¶ 76–77, 83, 151 (discussing "spillover" effects of open Internet).

management justification.[93] Such practices might indeed have posed serious public policy concerns about Internet fragmentation had they been common. But except for a few well-publicized incidents many years ago, ISPs in the U.S. have avoided content-based blocking or throttling, presumably because they see little commercial upside to the practice and much potential downside in the form of a consumer backlash and mass customer defections to fixed-line or mobile rivals.[94] Indeed, after the FCC rescinded the prohibitions on content-based blocking and throttling in 2017, no ISP to our knowledge began engaging in such practices, and all major ISPs publicly committed not to. Of course, the same market realities that reduce the *need* for no-blocking and no-throttling rules also reduce the *costs* of such rules, and for that reason such rules would likely survive a cost-benefit analysis.

Other net neutrality rules too, have typically mirrored rather than altered existing industry practices. Consider the virtual and then total ban on "paid prioritization" that the FCC imposed in separate orders issued in 2010 and 2015.[95] This highly touted prohibition had absolutely no effect on the broadband industry because, to our knowledge, no ISP engaged in the prohibited practices or had any plans to do so. Although the details often get lost in broad-brush rhetoric, the FCC always narrowly cabined this prohibition to avoid disrupting any of the techniques that broadband providers have actually used to "prioritize" latency-sensitive traffic. For example, the FCC studiously avoided banning ISPs from (1) accepting compensation for direct interconnection with content networks or (2) reserving dedicated capacity for IP-based multichannel video services over the same last-mile

93. *See Title II Order*, *supra* note 81, at 5646, ¶¶ 105–06.

94. *See* Mozilla Corp. v. FCC, 940 F.3d 72 (D.C. Cir. 2019) ("Petitioners do nothing to refute the agency's claim that 'since 2008, few tangible threats to the openness of the Internet have arisen.'") (quoting *RIF Order*, *supra* note 45, ¶ 113). For rhetorical effect, some advocates mischaracterize incidents that have nothing to do with net neutrality as episodes of "blocking" or "throttling." For example, they sometimes use the term "throttling" to describe the slower speeds that customers on tiered data plans sometimes experience after they have exceeded their monthly data allowances. But that practice has nothing to do with discriminating among content sources or preserving an open Internet, and it has always been lawful, even under the now-repealed Title II regime. *See Title II Order*, *supra* note 81, at 5668, ¶ 153 (recognizing that consumers should have lower-priced alternatives to unlimited data plans and that usage allowances, accompanied by lower speeds after those allowances are exceeded, "may benefit consumers by offering them more choices over a greater range of service options").

95. *See* Preserving the Open Internet, *Report & Order*, 25 FCC Rcd. 17905, para. 76 (2010), *aff'd in part and vacated in part*, Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014); *Title II Order*, *supra* note 81, ¶ 18.

pipes used for Internet access.[96] And when the FCC lifted the "paid prioritization" ban entirely in 2017, ISPs did not react by engaging in the narrow categories of non-existent conduct that were once prohibited. To the contrary, "paid prioritization," in the limited sense defined by the prior rules, remains a dead letter, presumably because existing, long-permitted network management practices have so far remained equal to the task of ensuring quality of service for latency-sensitive traffic.

b. All this said, aspects of the FCC's 2015 regime, announced in the *Title II Order*, did open the door to much more interventionist forms of regulation. The concern here lay not so much in the literal substance of the rules as initially adopted in 2015 as in their open-endedness and potential for regulatory creep.

Specifically, in asserting legal authority for the net neutrality rules discussed above, the *Title II Order* classified broadband as a Title II "telecommunications service" for the first time, ending more than a dozen years of broadband's classification as a mostly unregulated Title I "information service." Title II of the Communications Act applies to "common carriers" and subjects them by default to price controls and various other forms of economic regulation, although the FCC has broad authority to "forbear" from any Title II requirement that it deems inappropriate in particular contexts.[97] Of course, labels and roman numerals matter less than the actual details of a regulatory scheme. Title II classification can produce extremely interventionist regulation, as it did when applied to local exchange monopolies in the 20th century, or it can produce more permissive regimes, as it did when the FCC forbore from most forms of prescriptive regulation for mobile telephony services around the turn of the millennium.[98] The *Title II Order* itself claimed to follow the latter approach. For example, the FCC recognized that Title II classification exposed broadband ISPs to a threat of prescriptive rate regulation—*e.g.*, price caps—but disavowed any interest in

96. The FCC's *Title II Order* in 2015 defined "paid prioritization" as the compensated "management of a broadband provider's network"—*i.e.*, over last mile connections—"to directly or indirectly favor some traffic" exchanged over the public Internet—*i.e.*, across more than one IP network. *Title II Order*, *supra* note 81, ¶ 18 (italics omitted). ISPs have rarely if ever engaged in that practice, in part because it would present substantial engineering and collective-action challenges. *See* Nuechterlein & Weiser, *supra* note 15, at 208–09. At the same time, the *Title II Order* explicitly preserved all existing forms of IP traffic prioritization. For example, it declined to prohibit paid direct interconnection between ISPs and content delivery networks, which act as agents for their content provider customers. *See Title II Order*, *supra* note 81, ¶ 128. And it reaffirmed exemptions for "specialized" services, allowing ISPs to dedicate capacity for IP-based cable TV signals on the same pipes used for ordinary Internet traffic, thereby ensuring quality of service for ("prioritizing") the former but not the latter. *See Title II Order*, *supra* note 81, ¶¶ 207–13.

97. 47 U.S.C. § 160.

98. *See generally* Orloff v. FCC, 352 F.3d 415 (D.C. Cir. 2003).

such regulation and thus forbore from the relevant Title II provisions to the extent they would impose it.[99]

Despite these forbearance decisions, broadband ISPs expressed concern about the potential for regulatory creep now that the FCC had unlocked the legal mechanism for applying any form of common carrier regulation it deemed appropriate. Fueling those concerns was the FCC's concurrent decision in the *Title II Order* to adopt an amorphous "'no-unreasonable interference/disadvantage' standard," which supplemented the bright-line bans on blocking, throttling, and paid prioritization. This new rule prohibited broadband providers from "unreasonably interfer[ing] with or unreasonably disadvantag[ing] . . . end users' ability" to access edge providers or "edge providers' ability to make [their content or services] available to end users."[100] That prohibition was hardly self-revealing, and the FCC did not try to specify what types of conduct the ban might someday be found to forbid. Instead, the FCC announced a "non-exhaustive list" of seven nebulous factors it would use in applying this new rule, including "end-user control," "consumer protection," "effect on innovation," and "free expression."[101]

Industry concerns about how the FCC would apply this open-ended new rule grew in 2016, as it began investigating the "zero-rating" practices of mobile providers. Those investigations are worth recounting in some detail because they illustrate the phenomenon of regulatory creep in general and the elusive distinction between price and non-price regulation in particular.

Zero-rating arrangements ordinarily arise in the context of mobile data plans with designated usage allowances (*e.g.*, 10 GB per month). After a consumer reaches her allowance, the ISP typically charges her an overage fee or reduces her data speeds for the duration of the billing cycle. An ISP is said to "zero-rate" certain content if it excludes that content from a customer's data allowance. For example, AT&T offered tiered data plans that enabled its mobile customers to stream the content of its affiliate DirecTV on a zero-rated basis; although YouTube videos would count against their data allowances, online DirecTV streaming would not.[102]

In economic structure, a zero-rating arrangement is equivalent to a bundled discount. A consumer opting into such an arrangement is typically buying two products: a subscription to streaming content and a mobile broadband service. She pays both a subscription fee to the content provider and a wireless ISP bill that is discounted because it omits the overage fee the consumer *would* have paid as a result of streaming the provider's content in the absence of zero-rating. The consumer is indifferent as to how that discount is structured. Specifically, she does not care whether (1) her ISP charges her overage fees that the content provider then reimburses her for or (2) her ISP

99. *Title II Order*, *supra* note 81, ¶ 451–52. Notably, however, the FCC preserved the ability of private complainants to bring *ex post* challenges to particular broadband rates as "unjust" or "unreasonable." *Id.*

100. *Id.* ¶¶ 136–37 (italics omitted).

101. *Id.* ¶¶ 138–45.

102. Colin Gibbs, *Verizon, AT&T Questioned Over Zero-Rated Data*, FIERCE WIRELESS, (Dec. 2, 2016), https://www.fiercewireless.com/wireless/verizon-at-t-questioned-over-zero-rated-data [https://perma.cc/3QVX-AZZ3].

negates the overage fees but charges the content provider the same amount behind the scenes (through either a direct or imputed payment). Either way, the consumer receives a discount for her simultaneous purchase of both products. And such bundled discounts are generally procompetitive except in limited circumstances where a firm with substantial market power for one product can use them as a form of predatory pricing to exclude equally efficient providers of the other bundled product.[103] Absent such market power, bundled discounts pose no competition concerns at all: they are all consumer upside with no competitive downside.[104]

In autumn 2016, the FCC's staff, acting at the Chairman's direction, signaled that the agency would forbid many zero-rating arrangements as violations of the "no-unreasonable interference/disadvantage" rule.[105] It criticized such arrangements for encouraging consumers to view the video content zero-rated by a mobile carrier and thus deprived other providers of "a level playing field" when competing for the business of that carrier's mobile customers.[106]

This critique is difficult to understand from an economic perspective. Firms across the economy favor their affiliates and business partners over third parties all the time, and the government does not normally require them to give equal treatment to all other firms that might want it. For example, Walmart may preference its house brands over independent brands in terms of price or shelf space, but customers do not have to shop at Walmart; they can take their business to Target or to any other retailer, all of which preference their own house brands. Self-preferencing is generally viewed as an efficient form of product differentiation, at least in the absence of substantial market power.[107] Here, the FCC did *not* predicate its criticism of zero-rating plans on a finding that any of the relevant firms (*e.g.*, AT&T or

103. *See, e.g.*, Cascade Health Sols. v. PeaceHealth, 515 F.3d 883 (9th Cir. 2008).

104. *See generally* Stan J. Liebowitz & Stephen E. Margolis, *Bundles of Joy: The Ubiquity and Efficiency of Bundles in New Technology Markets*, 5 J. COMP. L. & ECON. 1 (2009).

105. *See* Letter from Jon Wilkins, Chief, FCC Wireless Telecomm. Bureau, to Robert W. Quinn, Jr., Senior Exec. Vice President, External & Legis. Affs., AT&T 1 (Dec. 1, 2016), https://cdn.arstechnica.net/wp-content/uploads/2016/12/Letter-to-R.-Quinn-12.1.16.pdf [https://perma.cc/FUD7-SK7J]. The staff distinguished between plans that zero-rated all content of a particular type (*e.g.*, music streaming) and those that zero-rated the content of affiliates or designated business partners. It appeared poised to condone the first practice and condemn the second. Notably, the AT&T "sponsored data" program criticized by staff offered third parties the opportunity to purchase zero-rating treatment at the same price at which DirecTV paid AT&T Mobility for it in the form of intra-corporate transfers, but staff dismissed that policy on the ground that such transfers are not equivalent to cash payments between independent third parties. *See id.* at 1–2. That position is questionable as an economic matter, but it is irrelevant to our argument here, which would apply whether or not an ISP offered third parties an opportunity to purchase sponsored data on the same terms as its content affiliate.

106. *See id.*

107. Net neutrality advocates often try to justify freestanding "nondiscrimination" rules on the ground that, without them, smaller firms would find it difficult to enter and grow. But the government does not typically require even dominant firms to accommodate undercapitalized new entrants that wish to compete with them. Instead, apart from programs administered by the Small Business Administration and similar agencies, it normally relies on the capital markets to give new entrants whatever financial resources they need to succeed if their products have commercial promise.

DirecTV) had market power in any relevant market (*i.e.*, mobile broadband or streaming content). Instead, the FCC expressed an essentially non-economic concern that these zero-rating arrangements violated abstract principles of neutrality. But the same could be said of bundled discount programs involving ISPs and their content affiliates, which the FCC had previously endorsed, [108] and which—as discussed—are economically equivalent to zero-rating arrangements and are almost always procompetitive in the absence of substantial market power.

Whatever the economic rationale, the FCC appeared to be taking the first steps towards regulating how ISPs charged consumers for broadband, despite prior assurances in the *Title II Order* that it would steer clear of rate regulation. That development coincided with advocacy for other types of regulation that also would have crossed the line into price regulation. For example, during this period, various consumer groups urged the FCC to restrict or prohibit tiered data plans altogether, effectively forcing ISPs to sell more unlimited-data plans and curbing any usage-sensitive component of retail broadband pricing.[109]

c. The emerging prospect of rate regulation by another name, along with the FCC's contemporaneous adoption of ISP-specific consumer privacy rules stricter than the FTC's generally applicable rules,[110] portended a major shift in U.S. broadband policy. Unlike the Title I regimes that preceded it, which largely codified existing industry practices, the new Title II regime now appeared likely to interfere with the settled business plans of broadband ISPs for the first time. That prospect was quickly overtaken by electoral events. In 2017, the FCC's new leadership pulled the plug on the zero-rating investigations and acted to restore broadband's prior classification as a Title I service,[111] while Congress nullified the broadband privacy rules under the Congressional Review Act.[112]

This history, however, teaches an enduring lesson about regulatory creep. The *Title II Order* of 2015 did not by its terms prohibit any existing ISP business practices; it adopted open-ended rules that might or might not have led to such prohibitions. Not until the following year did the FCC begin flexing its regulatory muscle to challenge prevailing practices. And when it did so, it appeared to open the door to some forms of rate regulation. Any ISP could reasonably have concluded in the fall of 2016 that this new common

108. *See* Applications of AT&T Inc. and DIRECTV for Consent to Assign or Transfer Control of Licenses and Authorizations, *Memorandum Opinion and Order*, 30 FCC Rcd. 9131, para. 4 (2015) [hereinafter *AT&T-DirecTV Merger Order*] ("[T]he combined AT&T-DIRECTV will increase competition for bundles of video and broadband, which, in turn, will stimulate lower prices, not only for the Applicants' bundles, but also for competitors' bundled products—benefiting consumers and serving the public interest.").

109. *See Title II Order*, *supra* note 81, ¶ 153, n.373 (citing advocacy and deferring decision on whether to impose restrictions on data caps).

110. *See* Protecting the Privacy of Customers of Broadband and Other Telecomm. Services, *Report and Order*, 31 FCC Rcd. 13911, para. 36 (2016).

111. *See generally RIF Order*, *supra* note 45.

112. *See* Pub. L. No. 115-22, 131 Stat. 88 (2017).

carrier regime would evolve in one direction only—towards greater regulatory intervention in the broadband marketplace, including through types of intervention, such as rate regulation, that the *Title II Order* seemed to disclaim.

Of course, sometimes regulation is necessary even if it tends to depress investment incentives on the margin. But any regulatory scheme should reflect an economically informed cost-benefit analysis that accounts for effects on investment incentives, and it needs to contain limiting principles to guard against economically *ill*-informed regulatory creep. The Title II regime fell short in those respects. Net neutrality regulation can be sensible if it is calibrated to prevent either anticompetitive (*i.e.*, welfare-reducing) conduct by dominant firms or conduct that genuinely threatens the Internet's status as an open, externalities-generating platform for communication, expression, and innovation. But the Title II regime applied to all ISPs indiscriminately without regard to market power. It ultimately prohibited conduct (such as zero-rating) that posed no threat to the basic openness of the Internet. And it championed poorly defined "neutrality" and "nondiscrimination" principles that fueled populist rhetoric and regulatory creep but were detached from serious economic analysis.[113] These are forms of regulatory overreach that we hope the FCC will avoid in future administrations.

C. State-Level Economic Regulation

We close this section by briefly noting the need for national consistency in any type of economic regulation for broadband. For decades, and until recently, policymakers of all political stripes agreed that basic decisions about such regulation should be set at the federal level and should not vary by state or locality. That consensus began in the 1970s and 1980s, when the FCC first preempted state regulation of online information services and the last-mile transmission services used to access them.[114] And the same consensus has appeared in every FCC order concerning open access and net neutrality, no matter where the order in question came out on the proper level of regulation as a general matter. For example, the relatively pro-regulation *Title II Order* announced the FCC's "firm intention to exercise [its] preemption authority to preclude states from imposing obligations on broadband service that are inconsistent with [its] carefully tailored regulatory scheme," including any state-level effort to "regulate the rates of broadband Internet access service."[115]

For the first time, the consensus favoring national consistency in economic broadband regulation has broken down. That is not because anyone

113. Notably, "Timothy Brennan, the [FCC's] chief economist at the time the [Title II] Order was initially in production . . . called [it] 'an economics-free zone.'" U.S. Telecom Ass'n v. FCC, 825 F.3d 764 (D.C. Cir. 2016) (Williams, J., dissenting in relevant part).

114. *See generally* California v. FCC, 39 F.3d 919, 931–33 (9th Cir. 1994) (describing FCC preemption decisions under the *Computer Inquiry* rules and upholding FCC preemption of state-level information service regulation, except as to purely "intrastate" services such as legacy voicemail).

115. *Title II Order*, *supra* note 81, at 5804, ¶ 433.

particularly welcomes state-by-state regulatory balkanization, but because critics of the FCC's current deregulatory approach have concluded that greater regulation at the state level is worth the price of such balkanization.[116] In our view, that position is short-sighted: if the current federal scheme is too permissive, the solution is to make it less so, not to open the door to 50 different schemes of state-level Internet regulation.

The Internet is designed by its nature to transcend geographic and political boundaries.[117] In a variety of contexts, state-by-state regulation would lead to intractable implementation problems. Internet peering agreements offer one instructive example. As discussed in Section III.B.3, the FCC has declined for decades to regulate the terms of interconnection arrangements between ISPs and the Internet's other constituent networks, leaving those arrangements instead to market forces. Now suppose that a state reaches a contrary policy conclusion and decides to regulate interconnection arrangements on a state-level basis for the first time. Would that state-level regulation apply (1) only to interconnection arrangements physically located within the state or (2) to all interconnection arrangements, wherever located, that might affect traffic flows within the state? Under the former approach, the restricted geographic scope of each state's scheme would artificially induce network operators to alter the Internet's physical architecture, not for sound engineering reasons, but simply to avoid (or take advantage of) state-level regulation. But under the latter approach, any state with the most interventionist scheme would effectively set regulatory policy for all states, given that centralized interconnection arrangements can affect traffic flows in many states.

More generally, state-by-state (or locality-by-locality) Internet regulation would likely have one of two consequences: (1) a regime in which industry participants must inefficiently rearrange their operations to conform to the disparate rules of many different states or (2) a regime in which the state or locality with the most interventionist approach sets nationwide policy by default, even if there is a consensus elsewhere that the state's approach is unduly burdensome. Either outcome would be highly undesirable. Again, if federal regulation is inadequate in some respect, the proper remedy is to modify it, not to fill the perceived regulatory gap with a state-by-state hodgepodge.

116. *See, e.g.*, Tom Wheeler, *Opinion: California Will Have an Open Internet*, N.Y. TIMES (Oct. 2, 2019), https://www.nytimes.com/2019/10/02/opinion/net-neutrality-fcc-wheeler.html [https://perma.cc/DB4P-UUD6].

117. *See generally* Am. Booksellers Found. v. Dean, 342 F.3d 96, 103–04 (2d Cir. 2003) (it is "difficult, if not impossible, for a state to regulate internet activities without 'project[ing] its legislation into other states,'" and such activities as a categorical matter may thus fall "within the class of subjects that are protected from State regulation because they 'imperatively demand[] a single uniform rule'") (alterations in original) (quoting Healy v. Beer Inst., 491 U.S. 324, 334 (1989), and Cooley v. Bd. of Wardens, 53 U.S. 299, 319 (1852)).

IV. RECONCILING COMPETITION POLICY WITH SOCIAL EQUITY

As discussed, private enterprise, subject only to light-touch oversight, invested the $1.7 trillion needed to transform the dial-up "worldwide wait" of the late 1990s into the world-class broadband experience most Americans enjoy today. And private enterprise is on the path to committing another trillion dollars (or more) in at-risk capital to deliver on the promise of ubiquitous gigabit connectivity for the next generation of Internet applications and devices. In this industry, as in most other dynamic markets characterized by substantial investment and innovation, the opportunity to earn profitable returns creates the high-powered incentives needed to produce the most value for the most consumers, efficiently and on a gigantic scale.

But speed, scale, and efficiency do not guarantee equity. Without governmental support, market forces alone will not solve the two greatest policy challenges of the coming decade: boosting (1) greater broadband *adoption* among low-income users, many of whom are priced out of online connectivity,[118] and (2) greater broadband *deployment* in sparsely populated areas, where unusually low economies of density can make private investment uneconomical in the absence of subsidies.[119] There is nearly universal consensus that the government should intervene to help close these twin digital divides—between rich and poor and between urban and rural. Those divides are more unacceptable than ever precisely because private industry has made the massive investments needed to convert high-speed Internet access from a discretionary luxury for a few into the pervasive communications platform it has become. What the *National Broadband Plan* observed in 2010 is all the more true today: "As more aspects of daily life move online and offline alternatives disappear, the range of choices available to people without broadband narrows. Digital exclusion compounds inequities for historically marginalized groups."[120]

The question is not *whether* government should intervene to meet these challenges, but *how* it should intervene. As we have discussed, the solution does not lie in rate caps, facilities-sharing obligations, or other forms of economic regulation, which would only make the problem worse by discouraging the private investment needed to expand broadband's reach. Instead, the way to close America's broadband gaps is the most obvious and direct one: the use of explicit subsidy programs to (1) reduce monthly broadband bills for low-income subscribers and (2) help broadband providers defray the costs of deployment in rural and other high-cost areas in exchange for commitments to provide specified levels of service in those areas.

The FCC has already laid the groundwork for these solutions by reorienting the focus of its longstanding universal service programs—Lifeline

118. *See generally* Lifeline & Link Up Reform and Modernization, *Third Report and Order*, 31 FCC Rcd. 3962, para. 5 (2016) [hereinafter *Lifeline Modernization Order*].

119. *See* Nuechterlein & Weiser, *supra* note 15, at 8–10, 307–14.

120. *National Broadband Plan*, *supra* note 2, at 129.

for low-income consumers and various support mechanisms for rural investment—away from voice telephone service towards broadband.[121] In the long run, however, Congress will need to revise the underlying statutory scheme to meet the challenges of 21st century communications. The existing statutory provisions governing "universal service," enacted before the advent of residential broadband, were drafted to support affordable dial-tone service by "eligible telecommunications carriers."[122] Although the FCC has found creative ways to square the statutory definition of that term with broadband-focused initiatives,[123] the language does impose real and arbitrary limits on the FCC's discretion. For example, it is by no means clear that the FCC could legally extend Lifeline support to anchor institutions, even if doing so is sometimes the most cost-effective means of increasing broadband adoption within low-income communities.[124] More broadly, closing the digital divide will require not only affordable *services*, but also affordable computing *devices*, along with greater levels of digital literacy in today's underserved communities.[125] These challenges, which post-date the telephone-centric "universal service" provisions of the Communications Act, all cry out for new federal legislation.

So, too, do the mechanisms for funding today's subsidy programs. Most of those programs are underwritten not by general tax revenues, but by mandatory "contributions" from telecommunications providers. These contributions are based on the providers' "interstate" revenues for specified services (mainly voice and data-transport) and are ultimately passed on to consumers in the form of increasingly bloated universal service fees, which appear as line items on telephone bills.[126] That system not only poses implementation issues of baroque complexity, but, worse, suppresses marginal demand for the assessed services by raising their effective price to consumers.[127] Indeed, the "contribution factor" on those services—in effect,

121. *See* Nuechterlein & Weiser, *supra* note 15, at 307–14 (describing replacement of High Cost Fund with Connect America Fund).

122. 47 U.S.C. § 214(e)(1), (6).

123. *See, e.g.*, *Lifeline Modernization Order*, *supra* note 119, ¶¶ 259–73.

124. *See* Jonathan Sallet, *Broadband for America's Future: A Vision for the 2020s*, BENTON INST. FOR BROADBAND & SOC'Y 67 (Oct. 2019), https://www.benton.org/sites/default/files/BBA_full_F5_10.30.pdf [https://perma.cc/V79J-5XMK] (explaining that the FCC "not[ed] a question about its legal authority" in 2016 to adopt proposals "to expand [Lifeline Broadband Provider status] . . . to community anchor institutions").

125. *See id.* at 64–77.

126. *See* Nuechterlein & Weiser, *supra* note 15, at 316, 321–25. Although in need of reform, today's contribution scheme is a major improvement over its predecessor. Under the schemes in place before the 1996 Act, incumbent telephone companies were expected to charge some customer groups—particularly business customers and households in metropolitan areas—rates far above the relatively low cost of serving them in order to subsidize below-cost rates for consumers who lived in higher cost areas. That "implicit subsidy" approach was unsustainable once competition emerged and new entrants cherry-picked the urban customers who would otherwise pay above-cost rates to the erstwhile monopolists. *See id.* at 298–300.

127. *Id.* at 316, 321–25.

an excise tax—has now swelled to 31.8%.[128] Such product-specific assessments might make sense where the government *wishes* to suppress demand, as in the case of taxes on alcohol or tobacco. But they make no sense when the objective is to *increase* demand and output in the communications sector. Congress appears to have recognized this point when it relied on general tax revenues to underwrite the broadband subsidies administered by the Departments of Agriculture and Commerce.[129] But the most important broadband subsidy programs are those administered by the FCC, and it is time for Congress to replace existing contribution mechanisms for those programs with general tax revenues as well.

Finally, however universal service programs may evolve, policymakers should continue to harmonize them with sound competition policy. Broadband subsidies can raise serious competition policy concerns if they are implemented without competitive neutrality in mind—for example, if they are disbursed to one provider but not to its rivals in the same market. In effect, these subsidies require consumers or taxpayers generally to pay for services most of them do not receive while disadvantaging firms that receive no subsidies and must therefore recover all of their costs from their own actual customers. This competitive bias distorts price signals and impairs market efficiency: a less efficient but subsidized ISP can easily win more business than a more efficient but unsubsidized ISP simply by charging less to its actual customers and forcing other consumers, who are *not* its customers, to make up the difference. That arrangement would also threaten to reduce competition if the downward pricing pressure created by subsidized entry keeps unsubsidized firms from recovering the costs of new investments. Carried to its logical conclusion, such asymmetric subsidies would leave no firms in the market other than the ones that rely most heavily on compulsory subsidies from consumers to whom they are not accountable.

This point may seem obvious, but it sometimes gets lost in policy debates about municipal broadband networks. Such a network can offer invaluable consumer benefits in many circumstances—for example, where it is the only broadband ISP in a market, or where it does not materially rely on taxpayer dollars or other exogenous sources of revenue (such as monopoly electric utility fees) to fund its operations. Concerns can arise, however, when

---

128 PROPOSED FIRST QUARTER 2021 USF CONTRIBUTION FACTOR, DA 20-1480 (Dec. 14, 2020), https://docs.fcc.gov/public/attachments/DA-20-1480A1.pdf ("[T]he proposed universal service contribution factor for the first quarter of 2020 is 0.318 or 31.8 percent.").

129. *See Reconnect Loan and Grant Program: Program Overview*, U.S. DEP'T OF AGRIC., https://www.usda.gov/reconnect/program-overview (last visited Sep. 20, 2020) [https://perma.cc/VB55-WE24] (noting that 2018 legislation "appropriated a budget authority of $600,000,000 to be used on an expedited basis"); *Broadband Technology Opportunities Program (BTOP) Quarterly Program Status Report*, U.S. DEP'T OF COM. 1 (July 2017), https://www.ntia.doc.gov/files/ntia/publications/ntia_btop_33rd_qtrly_report.pdf [https://perma.cc/92FD-N4TJ] (noting that the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, "appropriated $4.7 billion for NTIA to establish BTOP [the Broadband Technology Opportunities Program] to increase broadband access and adoption; provide broadband access, training and support to schools, libraries, healthcare providers, and other organizations; improve broadband access to public safety agencies; and stimulate demand for broadband").

municipal broadband networks both compete with private ISPs and receive material subsidies that those private ISPs do not. For example, one prominent advocate of "publicly incentivized competition" in "localit[ies] with an existing network" appears to support subsidies for new entrants but not incumbents competing in the same market.[130] In his view, "what some call 'overbuilding' should be called by a more familiar term: 'Competition.'"[131] In fact, competitively biased subsidy schemes are most aptly described by a different term: "predation." By shifting a portion of cost-recovery from users to taxpayers, they may create attractively low—*i.e.*, predatory—retail prices in the short term. But over the longer term, they suppress the investment incentives of all unsubsidized competitors and potentially drive them from the market, leaving taxpayers holding the bag.

An analogy helps illustrate the irrationality of such schemes. Suppose that a rural town with a lone country store wants to attract new retailers. But rather than achieving that objective through competitively neutral tax incentives, the town decides to open its own store and starts selling products at below-cost prices subsidized by tax revenues, in competition with the incumbent country store. Such predatory pricing might be politically popular for a time, but eventually the incumbent would close up shop, the government store would be the only retailer in town, and market forces would give way to taxpayer-supported central planning. Policymakers should bear similar concerns in mind when contemplating competitively asymmetric subsidies for municipal broadband systems.

* * *

Broadband policy debates tend to generate more heat than light, and many end in online flame wars. That is unfortunate because the participants usually have similar policy objectives. Almost everyone wants to promote broadband deployment, to see more facilities-based competition, to maintain an open Internet, and to close the digital divides between rich and poor and urban and rural. The debate is instead about the proper means to those ends.

By any meaningful metric, the U.S. broadband market is more vibrant and competitive than most of its foreign counterparts. Not coincidentally, it has become so without the substantial economic regulation that many of those counterparts have implemented. We would continue that light-touch approach and supplement it with limited types of regulatory intervention that survive an economic cost-benefit analysis, such as baseline net neutrality rules and competitively neutral subsidy programs. Perhaps more aggressive forms of economic regulation will someday become warranted. But the burden is on the proponents of such regulation to justify it—not by populist rhetoric, but by a genuine cost-benefit analysis of their own. In particular, they will need to identify a genuine market failure, explain why less interventionist approaches are inadequate to the task, and show that the benefits of their proposed solution outweigh the costs, including the investment-chilling costs

130. Sallet, *supra* note 125, at 32–33.
131. *Id.* at 32.

of regulatory uncertainty and creep. Until then, what Bill Kennard said two decades ago still holds: "We have to get these pipes built. But how do we do it? We let the marketplace do it."[132]

132. Kennard, *supra* note 7, at 4.

Erasing Transgender Public Figures' Former Identity with the Right to Be Forgotten

Hunter Iannucci*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School; B.A., Law & Society, May 2017, The American University. I would first like to thank Professor Dawn C. Nunziato, who helped inspire this Note and, more importantly, who encouraged me to write about what I believe in. Thank you to my friends for their relentless support of my fondness of going against the grain. Without all of you, I would not have survived the last three years of law school. Lastly, I would like to dedicate this Note to my father, whose biggest dream was witnessing my journey to becoming an attorney. Though you won't be around to see it, I know I've already made you proud.

I. INTRODUCTION

The name Zeke Smith may sound familiar: you might know him as the first transgender contestant on the popular CBS show *Survivor*. Less well known are the facts that he joined the show partly out of desire to validate his gender identity and that a fellow contestant torpedoed this desire by outing him as transgender on live television.

Zeke Smith began watching *Survivor* while coping with depression during his transition.[1] Transitioning was difficult for Zeke because, in his words, "the world doesn't treat trans people with much kindness," and it was only when his transgender identity was no longer widely known that he began to connect with others "in a meaningful way."[2] Zeke kept his gender identity a secret largely because "if [he] let anyone too close, they'd smell [his] stench and not want to be [his] friend anymore."[3]

It was not until Zeke became a *Survivor* contestant that he felt confident in his gender identity: "the moment I put . . . the official *Survivor* player uniform[] on . . . my confidence became real . . . I'd conquer whatever the game might throw at me. I was free."[4] Zeke decided "[not to] discuss [my] trans status . . . because I wanted the show to desire me as a game player . . . not as 'The First Trans *Survivor* Player.'"[5] But Zeke's costar, Jeff Varner, annihilated Zeke's newfound confidence by exposing him as transgender on live television by asking: "Why haven't you told anyone you're transgender?"[6] Zeke said he sat there "in a trance," feeling nothing but utter pain and shock.[7] On being outed, Zeke said:

1. *See* Lisa Respers France, *Zeke Smith Outed as Transgender on 'Survivor'*, CNN ENT. (Apr. 13, 2017, 8:35 PM), https://www.cnn.com/2017/04/13/entertainment/zeke-smith-transgender-survivor/index.html. [https://perma.cc/VPD2-H9YB].
2. Zeke Smith, *'Survivor' Contestant Opens up About Being Outed as Transgender (Guest Column)*, THE HOLLYWOOD REP. (Apr. 12, 2017, 9:00 PM), https://www.hollywoodreporter.com/live-feed/survivor-zeke-smith-outed-as-transgender-guest-column-991514 [https://perma.cc/D4K5-XPDV].
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. Smith, *supra* note 2.

> I'm not wild about [viewers] knowing that I'm trans. An odd sentiment, I realize, for someone who signed up for two seasons of the CBS reality giant, *Survivor* . . . when I got on a plane to Fiji last March, I expected to get voted out . . . I'd return home, laugh at my misadventure, and go about my life, casually trans in the same way that Zac Efron is casually Jewish.[8]

Despite Varner's profuse online apology, it did not ameliorate what he stole from Zeke in exposing his transgender status: his privacy.[9] As Zeke explained, "a person's gender history is private information and it is up to them, and only them, when, how, and to whom they choose to disclose that information."[10]

This anecdote about Zeke Smith underscores that a transgender person's ability to actualize their[11] gender identity requires the complete abdication of their former selves, which creates a unique privacy interest in maintaining the confidentiality of their birth names[12] and assigned sex at birth.[13] Revealing this personal information[14] exposes transgender persons to stigma and violence and threatens their ability to fully realize their gender identity.

However, U.S. privacy law is inadequate in guarding against the disclosure of transgender public figures' personal information. Public figures as a class are rarely successful in bringing actionable privacy claims given the emphasis courts place on accessibility to information concerning individuals with public-facing lives. On the off chance a public figure succeeds in their claim, the available legal remedies cannot completely rectify the harm done, for there is no legal mechanism that enables them to claw this sensitive

---

8. *Id.*

9. *See* Jeff Varner (@jeffvarner), TWITTER (Apr. 12, 2017, 9:11 PM) https://twitter.com/JEFFVARNER/status/852328280095109120 [https://perma.cc/ZN92-GFFJ].

10. *See* France, *supra* note 1.

11. This Note uses singular "they, them, theirs," instead of the pronouns "she, her, hers" or "he, him, his" to respect the gender identities of transgender individuals, as well as all other identities within the gender non-conforming community.

12. This Note uses "birth name" and "legal name" interchangeably. Both refer to the name given to transgender individuals at birth, as opposed to their chosen names that reflect their gender identity. Another term used to refer to transgender individuals' birth names are their "deadnames." Using a transgender individuals' birth name or legal name instead of their chosen name is to "deadname" them, a hostile act aimed at undermining their gender identity. Adrien Converse, *What Does "Deadname" Mean?* DECONFORMING, https://deconforming.com/deadname/ (last visited Dec. 28, 2020) [https://perma.cc/DTU8-MBSQ].

13. The term "assigned sex at birth" (hereinafter "ASAB") refers to the label a doctor gives a person at birth, primarily based on medical factors, including a person's hormones, chromosomes, and genitals. When discussing someone's sex, the appropriate term is "assigned female at birth" or "assigned male at birth." *See Sex, Gender, and Gender Identity*, PLANNED PARENTHOOD, https://www.plannedparenthood.org/learn/sexual-orientation-gender/gender-gender-identity (last visited Dec. 20, 2020) [https://perma.cc/LVD2-8BJG].

14. When the term "personal information" is used in reference to transgender individuals, it means their legal names and ASAB.

information back from the public's view. This legal reality, coupled with the need of transgender individuals to keep their personal information confidential, creates a distinct issue for the case of a transgender public figure seeking to sanction revelation of this information in online publications.

The United States should look to the European Union's "right to be forgotten" (RTBF) for guidance because, compared to the U.S., the EU favors more robust privacy protections—even in the face of competing press and speech freedoms.[15] If adopted, the RTBF's delisting mechanism would enable transgender public figures to request the removal of online articles referencing their personal information and redaction of their personal information. This remedy is essential to respecting the unique privacy interest arising from the transgender identity, which outweighs First Amendment speech and press freedoms for two reasons. First, implementing this remedy would only alter privacy law for a tiny population subset, as transgender individuals make up less than 1% of the U.S. population[16]—meaning this change would do little in the aggregate to upset privacy jurisprudence. Second, in adopting this solution, the American legal system stands to protect transgender persons from rampant stigmatization, discrimination, and physical violence, which could play a significant role in combatting efforts to vitiate federal legal protections for transgender individuals, such as those that occurred under the Trump administration.[17]

Part II begins in Section A with an overview of the unique privacy interest encompassed by the transgender identity. Section B examines the tort of public disclosure as a mechanism to enforce privacy rights, noting the tort's inapplicability to "newsworthy" information, which is information of such

---

15. The right to be forgotten (hereinafter "the RTBF") refers to a legal mechanism created by the European Court of Justice in *Google Spain SL v. Agencia Espanola de Proteccion de Datos* (*Google Spain*) designed to enforce privacy rights. The RTBF enables individuals (usually referred to as data subjects in this context) to request data controllers, like Google, to remove links resulting from searches for their names when those results are "inadequate, irrelevant, or excessive in relation to the purposes for which they are collected." *See* Dawn C. Nunziato, *The Fourth Year of Forgetting: The Troubling Expansion of the Right to be Forgotten*, 39 U. PA. J. INT'L L. 1011, 1014 (2018) (citing 2014 E.C.R. Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzalez, 317, para. 94, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131 [https://perma.cc/6X2F-6PCW] (hereinafter *Google Spain*)).

16. In 2016, less than 0.6% of the U.S. population identified as transgender. *See* Andrew R. Flores, et al., *How Many Adults Identify as Transgender in the United States?*, WILLIAMS INST. 3 (June 2016), https://williamsinstitute.law.ucla.edu/publications/trans-adults-united-states/ [https://perma.cc/78GM-N4ME].

17. Sandy E. James et. al, *The Report of the 2015 U.S. Transgender Survey*, NAT'L CTR. FOR TRANSGENDER EQUAL. 4–5 (Dec. 2016), https://www.transequality.org/sites/default/files/docs/USTS-Full-Report-FINAL.PDF [https://perma.cc/LZ3R-AMDF]; Lola Fadulu, *Trump's Rollback of Transgender Rights Extends Through Entire Government*, N.Y. TIMES (Dec. 6, 2019), https://www.nytimes.com/2019/12/06/us/politics/trump-transgender-rights.html [https://perma.cc/95J2-XAFT].

concern to the public it overrides a person's privacy interests or concerns an innately newsworthy person because they occupy a prominent role in public life and thus are considered a public figure. Section B explains that on the rare occasion when public figures succeed in making public disclosure claims, legal remedies are insufficient to rectify the harm done, which creates an obstacle for transgender public figures seeking to ban publication of their personal information. Section C introduces the EU's RTBF as a solution, positing the EU's privacy protections as instructive in resolving this issue.

Part III imports the RTBF to resolve the issue. Section A cements privacy law's failure to protect transgender public figures' personal information while finding the RTBF equipped to do so. Section B asserts that the RTBF comports with First Amendment freedoms, and further that certain legal mechanisms already act as blueprints for creating an American right of erasure. Finally, this Note concludes with a cursory overview of what implementation would look like, arguing in favor of federal legislation to codify this solution.

II. BACKGROUND

A. The Transgender Identity and Privacy Rights

Being transgender entails the complete abdication of an individual's former gender identity. The term itself embraces not only a difference in gender identity, but a personal metamorphosis: a transgender individual's "gender [identity] and [expression] [does] not conform to the gender they were assigned at birth."[18] A transgender individual may have made "social, medical, or surgical steps to physically or socially bring their body or gender expression in line with the gender with which they identify."[19] These social, medical, and surgical steps are part of transitioning, a process integral to the expression of a transgender person's gender identity.[20] Transitioning is motivated by a desire to compel the world to validate a transgender person's

18. See JACKSON WRIGHT SHULTZ, TRANS/PORTRAITS: VOICES FROM TRANSGENDER COMMUNITIES 200–01 (2015). *See also Glossary*, LAMBDA LEGAL, https://www.lambdalegal.org/protected-and-served/glossary#Transfeminine (last visited Nov. 24, 2020) [https://perma.cc/P3NM-4WYY] ("Transgender: refers to people whose gender identity . . . differs from their assigned or presumed sex at birth"). This is not to suggest all transgender individuals express their identity the same ways. The transgender identity is complex and not monolithic, but the above provides a baseline definition for the purposes of this Note.

19. SHULTZ, *supra* note 18, at 200–01.

20. *See* Stephanie L. Budge et al. *Transgender Emotional and Coping Processes: Facilitative and Avoidant Coping Throughout Gender Transitioning*, 41 THE COUNSELING PSYCH. 601, 603–04 (2013) (Transitioning refers to transgender individuals who have "[undergone] medical intervention, but it can be used more inclusively . . . the word *transition* literally means 'to change' . . . *Transition* . . . refer[s] to the process . . . transgender individuals go through to identify as transgender.").

gender identity,[21] but also partly by the fear of being "found out,"[22] given the vulnerability of transgender persons to social stigma, discrimination, sexual assault, and physical attack.[23] Such discrimination has always been pervasive, but has become even more so in recent years under President Trump, as illustrated by the increase in violence against transgender persons since the beginning of 2017,[24] as well as the former Administration's efforts to rollback legal protections for transgender persons.[25]

There is ample research evincing the scope of discrimination and violence perpetuated against transgender persons—especially when their gender identity is exposed. The D.C. Office of Human Rights' (OHR) study, *Qualified and Transgender*, outlines employers' discriminatory responses to an applicant's transgender identity—specifically, the study shows

---

21. *See* Stacey M. Brumbaugh-Johnson & Kathleen E. Hull, *Coming Out as Transgender: Navigating the Social Implications of a Transgender Identity*, 66(8) J. OF HOMOSEXUALITY 1148, 1164 (2019). This comes from a study that examined transgender coming-out narratives. A transgender man explained that his decision to transition was done in part to compel his parents to validate his gender identity: "Steven said [his parents] still do not accept his identity. He expressed uncertainty about his parents' response to his next stages of transitioning: 'So, I think it'll be very interesting once I'm really beyond the point of no return in terms of low voice and beard and all that kind of thing . . . how they'll react to that, because then they really can't pretend anymore.'"

22. *Id.* at 1163. A transgender woman discussed her transition: "I wanted my transition to be complete . . . I didn't want to have that fear . . . [or] be worried [that] . . . somebody might figure it out. Somebody might know who I am."

23. James, *supra* note 17, at 4–5. (Transgender respondents reported severe discrimination in all aspects of life; 10% who were out to their family reported experiencing violence committed against them by their family because they were transgender; 8% were kicked out of their house because they were transgender. Of the respondents who were out as transgender in school, 54% were verbally harassed; 24% were physically attacked; 13% were sexually assaulted; and 17% left school because of mistreatment. Of the respondents that were out as transgender at work, 30% reported mistreatment at work due to being transgender, including being fired, denied a promotion, or physical or sexual assault).

24. *See, e.g.*, *Fatal Violence Against Transgender People in America 2017*, HU. RTS. CAMPAIGN 4 (2017), http://assets2.hrc.org/files/assets/resources/A_Time_To_Act_2017_REV3.pdf [https://perma.cc/W9P5-YS49] (finding 25 transgender persons were murdered since Trump's election in 2016); *Murders of Transgender People in 2020 Surpasses Total for Last Year in Just Seven Months*, NAT'L CTR. FOR TRANSGENDER EQUAL., (Aug. 7, 2020) https://transequality.org/blog/murders-of-transgender-people-in-2020-surpasses-total-for-last-year-in-just-seven-months [https://perma.cc/GSR2-86KE] (indicating violence against transgender persons increased from 2019 to 2020, with the number recorded "surpass[ing] the total for all of 2019"—that is, 28 transgender individuals lost their lives as of August 2020 as compared to 26 in 2019.).

25. Fadulu, *supra* note 17 (outlining how President Trump rolled back legal protections for transgender individuals, including the transgender military ban, the Department of Health and Human Services' proposal to vitiate the Affordable Care Act's ban on discrimination against transgender individuals in healthcare, the Justice Department's reduction of protections for transgender individuals in prisons, and the Department of Housing and Urban Development's attempts to rollback protections for transgender individuals in homeless shelters).

transgender persons face substantial hurdles in the hiring process, as evidenced by employers' selection of less qualified, cisgender[26] applicants over more qualified transgender applicants.[27] Similarly, Professor Cynthia Lee's article, *The Trans Panic Defense Revisited*, denotes the grave consequences of suddenly exposing a transgender individual's identity by outlining the "transgender panic defense," a criminal defense strategy asserted by a cisgender male defendant charged with murdering a transgender woman.[28] It is used as a provocation defense, where a male defendant claims upon discovering the victim was not biologically female but transgender, he became so enraged that he committed the murder because he lost control of himself, and thus should be convicted of a lesser offense, like voluntary manslaughter.[29] The defense originates from society's hostile belief that it is the transgender woman's fault for supposedly "deceiving" the defendant about her gender identity,[30] and when her gender identity is exposed, the natural response of anyone in the defendant's position would be violence.[31] This deeply entrenched belief that violence against transgender individuals is justifiable denotes the need for heightened legal protections of transgender individuals' personal information to shield them from violence. Professor Lee's research indicates both that transgender individuals have a privacy interest in safeguarding their personal information from the public, and that recognition and protection of this distinct privacy interest is integral to shielding them from stigma, violence, and their right to be free from discrimination on the basis of their gender identity.

However, the interest in maintaining the confidentiality of their personal information does not vanish when a transgender individual becomes "newsworthy" if they are considered a public figure.[32] In fact, transgender public figures are even more vulnerable to the effects of such disclosure because public figures are often unable to seek redress for exposure of private

---

26. "Cisgender" describes individuals whose gender identity aligns with their assigned sex at birth. *See* Cynthia Lee & Peter Kwan, *The Trans Panic Defense: Masculinity, Heteronormativity, and the Murder of Transgender Women*, 66 HASTINGS L.J. 77, 90 (2014).

27. Teresa Rainy & Elliot E. Imse, *Qualified and Transgender*, D.C. OFF. HU. RTS. 6 (2015), https://ohr.dc.gov/sites/default/files/dc/sites/ohr/publication/attachments/QualifiedAndTransgender_FullReport_1.pdf [https://perma.cc/DJ8F-QK8N] (finding 48% of employers preferred at least one less-qualified cisgender applicant over a more qualified transgender applicant; 33% of employers extended interviews to one or more less-qualified cisgender applicants over a more qualified transgender applicant).

28. Cynthia Lee, *The Trans Panic Defense Revisited*, 57 AM. CRIM. L. REV. 1411, 1411 (2020).

29. *Id.*

30. *Id.* at 1436–38 (citing People v. Merel, No. A113056, 2009 WL 1314822, at *6–9 (Cal. Ct. App. May 12, 2009)).

31. *See* Lee, *supra* note 28, at 1436.

32. *Cf.* Wasser v. San Diego Union, 191 Cal. App. 3d 1455, 1462 (1987) (quoting William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 418 (1960)) (affirming the principle that once a person becomes a public figure, the details of their lives and of "'past events . . . can properly be a matter of present public interest,'" and that "'one quite legitimate function of the press is . . . educating . . . the public as to [that] past history'").

information.[33] Moreover, even when public figures are successful in bringing an invasion of privacy claim, civil liability does not adequately remedy the potential harm of such a revelation. Remedies usually take the form of monetary damages, which do not resolve the harm suffered, because no dollar amount can offset the disruption to a transgender person's life when another publicizes their information.[34] Nor is there a dollar amount that can offset the danger of being exposed to violence and stigma.[35]

Injunctive relief—whereby a court orders an injunction to restrain publication of information—is also an available remedy.[36] However, injunctive relief does little to remedy the harm done if publication has already occurred. While a court can restrain further publication, once the proverbial cat is out of the bag, there is no way to delete information from the public's view once it is published online.[37]

Understanding why privacy law is inadequate to rectify the harm done by publicizing a transgender public figure's personal information requires understanding the limits of U.S. privacy law—specifically, how First Amendment speech and press freedoms restrict informational privacy rights.

B. Privacy Law: Informational Privacy Rights Versus the First Amendment in the Tort of Public Disclosure

The notion a person has the right, within certain bounds, to maintain control over dissemination of their personal information is the cornerstone of

33. *See* Sipple v. Chron. Publ'g Co., 154 Cal. App. 3d 1040, 1049–50 (1984) (quoting the RESTATEMENT (SECOND) TORTS § 652D cmt. g (AM. L. INST. 1977)) (finding public figures are "regarded as properly subject to the public interest, and publishers are permitted to satisfy the curiosity of the public as to its heroes, leaders, villains and victims, and those who are closely associated with them.").

34. *See* Diaz v. Oakland Trib., Inc., 139 Cal. App. 3d 118, 136 (1983). *See, e.g.*, Budge, *supra* note 20, at 604.

35. *See, e.g.*, Lee, *supra* note 28, at 1422; Abby Elin, *For Transgender Women, an Extra Dose of Fear*, N.Y. TIMES (Aug. 9, 2017), https://www.nytimes.com/2017/08/09/well/mind/for-transgender-women-an-extra-dose-of-fear.html [https://perma.cc/357U-PESH]; *Violence Against the Transgender Community in 2019*, HU. RTS. CAMPAIGN, https://www.hrc.org/resources/violence-against-the-transgender-community-in-2019 (last visited Dec. 28, 2020) [https://perma.cc/8AW9-B8SZ] (explaining in 2019, at least twenty-six transgender or gender non-conforming people were killed—an increase from 2018, in which there were at least twenty-two recorded murders of transgender individuals); *see also A National Epidemic: Fatal Anti-Transgender Violence in America in 2018*, HUM. RTS. CAMPAIGN, https://www.hrc.org/resources/a-national-epidemic-fatal-anti-transgender-violence-in-america-in-2018 (last visited Dec. 28, 2020) [https://perma.cc/4HS6-W93X].

36. *See, e.g.*, 37 CALIFORNIA FORMS OF PLEADING AND PRACTICE—Annotated § 429.392 (2019); Leavy v. Cooney, 214 Cal. App. 2d 496, 504 (1963); 4 TEXAS TORTS AND REMEDIES § 53.08 (2019).

37. *See* Garcia v. Google, 786 F.3d 733, 745 (9th Cir. 2015) (there is no right of erasure in the U.S. that allows a person to delete content from the Internet).

informational privacy.[38] The tort of public disclosure allows an individual to bring suit for invasion of privacy by alleging a defendant has publicized personal information that is private and highly sensitive.[39] However, the tort is largely restricted by First Amendment freedoms; this is because in assessing a defendant's liability for publicizing a plaintiff's personal information, courts will balance the plaintiff's need to assert control over their personal information against the public's interest in maintaining access to the information, as well as the press's right to print it.[40]

Samuel Warren and Louis Brandeis articulated the earliest iteration of a right to informational privacy in their law review article on a common law right to privacy, in which they stated there is a "right to be let alone" from unwarranted government intrusion into the privacy of one's home and life.[41] This was then codified in the Restatement (Second) of Torts as "one who gives publicity to . . . the private life of another."[42] Also dubbed the tort of public disclosure, this tort turns on whether information is "highly personal[,] representing the most intimate aspects of human affairs."[43] Remedies primarily take the form of monetary damages to compensate the plaintiff for the emotional pain caused by the disclosure of their personal information—including compensatory, punitive, and nominal damages, with types and amounts differing by state.[44] Injunctive relief is also available as a remedy.[45] When granted, it restrains further publication of the plaintiff's private information.[46]

Liability for the tort of public disclosure is triggered when (1) an individual publicizes a fact (2) that is private and (3) "highly offensive to a reasonable person," and (4) the public has no legitimate interest in this information.[47] These elements have been interpreted differently by lower courts, with only limited treatment by the Supreme Court.

---

38. *See* U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

39. *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977).

40. *See* Sean M. Scott, *The Hidden First Amendment Values of Privacy*, 71 WASH. L. REV. 683, 699–700 (1996) (summarizing Fla. Star v. B.J.F., 491 U.S. 524, 526 (1989)).

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

42. *See* RESTATEMENT (SECOND) OF TORTS § 652D.

43. Doe v. Luzerne Cnty., 660 F.3d 169, 176 (3d Cir. 2011).

44. *See Diaz*, 139 Cal. App. 3d at 136–37; *see, e.g.*, 1 LEXISNEXIS PRACTICE GUIDE: FLORIDA PERSONAL INJURY § 7.18 (2019) (Florida awards compensatory damages for invasion of privacy based on resulting injuries, but if evidence fails to show the plaintiff sustained a substantial injury, nominal damages may be granted; punitive damages may be awarded if there is a showing of defendant's "wantonness or recklessness"); 1 LEXISNEXIS PRACTICE GUIDE: PENNSYLVANIA PERSONAL INJURY § 2.17 (2019) (Pennsylvania awards nominal, compensatory, and punitive damages for invasion of privacy); 4 TEXAS TORTS AND REMEDIES, *supra* note 36 (Texas awards compensatory damages; nominal damages are awarded if the plaintiff cannot show the amount of loss; exemplary damages may be awarded if plaintiff suffered actual damage and proves defendant acted maliciously).

45. *See, e.g.*, 37 CALIFORNIA FORMS OF PLEADING AND PRACTICE—ANNOTATED § 429.392, *supra* note 36; 4 TEXAS TORTS AND REMEDIES, *supra* note 36.

46. *See, e.g.*, *Leavy*, 214 Cal. App. 2d at 504.

47. *See* RESTATEMENT (SECOND) OF TORTS § 652D.

The first element, publicity, requires a defendant to communicate a private fact to the public, regardless of the communication medium.[48] While the Restatement requires the communication be made to the public at large, the necessary *degree* of publicity varies across jurisdictions.[49] Some courts hold the communication must be made to a large number of individuals so the information is likely to become accessible to the general public.[50] Other courts construe it liberally and find communication to small subsets of the population satisfies the "publicity" criterion.[51]

The second element—whether information is "private"—turns on whether information is already in the public domain.[52] As such, information in public records is not private, so a person's birth date, military status, or pleading filed in a lawsuit are not private facts.[53] This is referred to as the "public records exception," which the Supreme Court outlined in *Cox Broadcasting Corp. v. Cohn*. In that case, the Supreme Court held that televising a deceased sexual assault victim's name was not actionable because the broadcaster obtained this information through publicly available court records.[54] So, when is information private? The Restatement elucidates that everyone has aspects of their lives they do "not expose to the public eye, but [keep] entirely to [themselves] or at most [reveal] only to . . . family or to close friends."[55] The Restatement lists sexual relationships, serious illnesses, and family quarrels as "intimate details" that, if revealed, may constitute an actionable invasion of privacy.[56]

The third element—whether the information disclosed is "highly offensive"—is a question of fact, which requires considering whether the average person would find revelation of the facts at issue to be offensive in context.[57] Courts have held that the disclosure of a person's HIV status or sexual orientation to a large number of people to constitute publicity of a

48. *See id.* cmt. a.

49. *See id.*

50. *See* St. Anthony's Med. Ctr. v. H. S. H., 974 S.W.2d 606, 610 (Mo. Ct. App. 1998) (the publicity element requires the communication be made "to the public in general or to a large number of persons" as opposed to just one or a few individuals).

51. *See*, *e.g.*, Hillman v. Columbia Cty., 474 N.W. 2d 913, 920 (Wis. Ct. App. 1991) (holding a prison guard communicating a private fact—an inmate's HIV-positive status—to other guards and inmates constituted publicity).

52. *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. b.

53. *See id.*

54. *See* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 495 (1975).

55. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b.

56. *Id.*; *see also* 1 LEXISNEXIS PRACTICE GUIDE: PENNSYLVANIA PERSONAL INJURY § 2.17, *supra* note 44 ("Inherently private facts include a person's financial, medical, or sexual life.").

57. *See* Pontbriand v. Sundlun, 699 A.2d 856, 865 (R.I. 1997); *see also* RESTATEMENT (SECOND) OF TORTS § 652D cmt. c. (noting that this inquiry will be relative to the customs and values of society).

highly objectionable kind.[58] Generally, this element turns on whether publication of the information would cause emotional distress or embarrassment to the average person.[59]

That said, even when facts are private, highly offensive, and are communicated with sufficient publicity, a plaintiff's public disclosure claim may still be defeated by the fourth element—the newsworthiness exception—if the information is deemed newsworthy. Information is newsworthy if it is central to the public's interest, either because the fact itself is of public importance, or the plaintiff occupies such a significant role in public life that they are of public importance.

1. Limiting the Public Disclosure Tort: The Newsworthiness Exception

The newsworthiness exception limits the public disclosure tort in that it requires weighing a person's privacy interest against speech and press freedoms.[60] This balance between privacy rights and First Amendment freedoms has teetered towards the latter, and over time, the newsworthiness exception has become so powerful it has "[swallowed] the tort."[61]

The Supreme Court has done little to clarify the contours of newsworthiness. It only referenced the newsworthiness exception in two cases, *Cox Broadcasting Corp. v. Cohn* and *Florida Star v. B.J.F.*, but failed to directly address whether the information at issue in both cases was

58. *See* Simpson v. Burrows, 90 F. Supp. 2d 1108, 1125, 1132 (D. Or. 2000) (finding disclosure of plaintiff's sexual orientation to a large number of people by mailing letters to public institutions revealing plaintiff was an "immoral" and "perverted" lesbian constituted revealing of facts in a manner that would be highly offensive to a reasonable person); *see also* Urbaniak v. Newton, 277 Cal. Rptr. 354, 360 (Ct. App. 1991) (holding the disclosure of plaintiff's HIV-positive status was actionable, as HIV was "ordinarily associated either with sexual preference or intravenous drug uses" and was, although should not have been, "viewed with mistrust or opprobrium," and thus disclosure would be highly offensive to a reasonable person).

59. *See* Prosser, *supra* note 32.

60. *See, e.g.*, Gill v. Hearst Pub. Co., 40 Cal. 2d 224, 228 (1953); *Cox Broad. Corp*., 420 U.S at 489.

61. Harry Kalven, Jr., *Privacy in Tort Law: Were Warren & Brandeis Wrong?*, 31 L. & CONTEMP. PROBLEMS, 326, 336 (1966).

newsworthy per se.[62] Given the Supreme Court's limited guidance, lower courts have found a variety of subject matter newsworthy.[63] Professor Richard Karcher surveyed the different tests employed by various courts for newsworthiness,[64] including the Ninth Circuit,[65] Second Circuit,[66] and District of Columbia Court of Appeals.[67] Each test examines different instances in which the public's interest in information trumps (or does not trump) a plaintiff's privacy rights—particularly in the context of a public figure plaintiff. Although these newsworthiness tests differ in various respects, they all share one significant commonality: they each vitiate the tort's deterrent value by decreasing the likelihood courts will impose liability on media defendants.[68]

---

62. The facts of *Cox Broadcasting Corp. v. Cohn* and *Florida Star v. B.J.F* are similar. In *Cox*, plaintiff sued defendant for televising the name of a deceased sexual assault victim the defendant obtained from publicly available court records. *See Cox Broad. Corp.*, 420 U.S. at 473–74. In *Florida Star*, plaintiff sued a newspaper company for printing the full name of a rape survivor it obtained from a police report. *See Fla. Star*, 491 U.S. at 526. In both cases, the Court found publication of lawfully obtained, truthful information already in the public domain is protected by the First Amendment. *See Cox Broad. Corp.*, 420 U.S. at 471; *see also Fla. Star*, 491 U.S. at 541. Putting the onus on the state, the Court found the state had the power to restrict the public availability of this information. *See Cox Broad. Corp*, 420 U.S. at 497; *Fla. Star*, 491 U.S. at 540–41. The Court explained if the state did not affirmatively do so, it reflected the state's determination that the matter was of public concern, and therefore newsworthy, though it never directly addressed whether the information was per se newsworthy. *See Cox Broad. Corp*, 420 U.S. at 495; *Fla. Star*, 491 U.S. at 541.

63. *See, e.g.*, Walter v. NBC Tel. Network, Inc., 811 N.Y.S.2d 521, 523 (App. Div. 4th Dept. 2006) (comedic information is newsworthy); Hull v. Curtis Publ'g Co. 125 A.2d 644, 646 (Pa. Sup. Ct. 1956) (educational information is newsworthy).

64. *See* Richard T. Karcher, *Tort Law and Journalism Ethics*, 40 LOY. U. CHI. L.J. 781, 795–96 (2009).

65. *Id.* at 795 (quoting Capra v. Thoroughbred Racing Ass'n, 787 F.2d 463, 464 (9th Cir. 1986)). The Ninth Circuit designates three factors for juries to weigh in determining whether information is newsworthy: "(1) the social value of the facts published, (2) the depth of the publication's intrusion into ostensibly private affairs, and (3) the extent to which the [individual] voluntarily assumed a position of public notoriety."

66. *Id.* at 795 (citing Sidis v. F-R Pub. Corp., 113 F.2d 806, 809 (2d Cir. 1940)). The Second Circuit found publicizing truthful facts about public figures does not offend the average person's standards of decency, saying "the misfortunes and frailties of . . . 'public figures' are subjects of considerable interest and discussion to the rest of the population" and that courts should not bar discussion of such matters.

67. *Id.* at 796 (quoting Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580, 589 (D.C. 1985)). The Court of Appeals for the District of Columbia emphasized the First Amendment's role in the newsworthiness exception and its capability to bar public officials and even those who "attempted to avoid publicity" from seeking redress for publicizing information concerning "interesting phases of human activity and . . . information . . . appropriate so that an individual may cope with the exigencies of their period."

68. *Id.* at 796.

2. The Newsworthiness Exception and Public Figures

The Supreme Court defines public figures as those who garner public attention either by occupying "positions of . . . pervasive power and influence" or thrusting "themselves to the forefront of particular public controversies."[69] Lower courts have deemed a variety of individuals public figures: celebrities,[70] government officials,[71] criminals,[72] inventors,[73] and even individuals who become public figures unwillingly (such as an individual present at the scene of a crime).[74] Public figures are believed to have given up a range of privacy rights in "voluntarily acced[ing] to a position of public notoriety."[75] So long as the subject matter is true and newsworthy in that it captures the public's legitimate interest, courts generally side with publications—even in cases where the intrusion into private life appears excessive.[76] Because the First Amendment protects robust debate on public issues, courts find that even serious intrusions into a public figure's life serve this interest.[77] The following section outlines the various approaches lower courts have taken to gauge the newsworthiness of public figures' personal information.

3. "Testing" the Newsworthiness of Public Figures' Personal Information

Lower courts apply different newsworthiness tests. The following cases apply a standard loosely paraphrasing the standard articulated by the Ninth Circuit in determining the newsworthiness of public figures' personal information, weighing three factors: (1) the social value of the information, or the relevance of the information to understanding the story told in the publication or public figure themselves; (2) the extent the publication intrudes

---

[69] Gertz v. Robert Welch, 418 U.S. 323, 345 (1974).

70. Shlomit Yanisky-Ravid & Ben Zion Lahav, *Public Interest vs. Private Lives—Affording Public Figures Privacy in the Digital Era: The Three Principle Filtering Model*, 19 U. PA. J. CONST. L. 975, 980 (citing Ann-Margret v. High Soc'y Mag., Inc., 498 F. Supp. 401, 404 (S.D.N.Y. 1980)).

71. *See id.* at 980–81 (citing *Gertz*, 418 U.S. 323, 345 (1974)).

72. *See id.* at 981 (citing Marcone v. Penthouse Int'l Mag. for Men, 754 F.2d 1072, 1085 (3d Cir. 1985)).

73. *See id.* (citing Thompson v. Curtis Publ'g Co., 193 F.2d 953, 954 (3d Cir. 1952)).

74. *See id.* (quoting *Gertz*, 418 U.S. at 345) ("Hypothetically, it may be possible for someone to become a public figure through no purposeful action of his own, but the instances of truly involuntary public figures must be exceedingly rare.").

75. *See generally* Kapellas v. Kofman, 1 Cal. 3d 20, 25 (1969).

76. *See, e.g.*, Jeffrey F. Ghent, Annotation, *Waiver or Loss of Right of Privacy*, 57 A.L.R. 3d 16, *5 (1974) (quoting Briscoe v. Reader's Dig. Ass'n, 4 Cal. 3d 529, 535 n.5 (1971)) ("Almost any truthful commentary on public officials or public affairs, no matter how serious the invasion of privacy, will be privileged."); Branson v. Fawcett Publ'ns, Inc., 124 F. Supp. 429, 433 (E.D. Ill. 1954).

77. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 281 (1964).

into a public figure's life; and (3) the degree to which the public figure willingly assumed a place in public life.[78]

In *Kapellas v. Kofman*, the Supreme Court of California applied these three newsworthy factors to decide whether the delinquent behavior of a politician's children was newsworthy.[79] There, Inez Kapellas, a political candidate, brought an invasion of privacy claim against a newspaper for an editorial denigrating her candidacy, stating her children's arrests reflected her poor parenting ability and political ineptitude.[80] First, the court found Kapellas' candidacy for public office made the information valuable because the public had a right to learn about "any facet of a candidate's life that may relate to [their] fitness for office."[81] Second, the court found the newspaper's conduct was justifiable and did not intrude into Kapellas's life.[82] Because the public had a right to information relevant to her candidacy, the press was allowed to have ample opportunity "to disseminate all information that may cast a light on a candidate's qualifications," making the intrusion permissible.[83] Also bearing on this factor was that her children's arrests were matters of public record and not confidential, minimizing the supposed intrusion into her private life.[84] Third, the court found Kapellas's participation in politics meant she voluntarily acceded to a position of prominence and thus knowingly subjected herself to a "searching beam of public interest and attention."[85] The court noted the salience of First Amendment freedoms in its decision, commenting the loss of Kapellas's children's privacy was "the cost[] of [retaining] . . . a free marketplace of ideas."[86]

Diaz v. Oakland Tribune diverges from the *Kapellas* court's approach to newsworthiness. Though the California Court of Appeals in *Diaz* decided a public figure's transgender identity was non-newsworthy, it reached this conclusion on weak footing. There, ToniAnn Diaz sued a newspaper for public disclosure of a private fact for publishing a story exposing her as transgender.[87] After changing her name and transitioning, Diaz kept her transgender identity secret.[88] Years later, while acting as her university's student body president, Diaz charged the school with fund misappropriation

78. *Capra*, 787 F.2d at 464 (designating three factors for the jury to weigh in determining whether information is newsworthy: "(1) the social value of the facts published, (2) the depth of the publication's intrusion into ostensibly private affairs, and (3) the extent to which the individual voluntarily acceded to a position of public notoriety.").
79. *See Kapellas*, 1 Cal. 3d at 24–25.
80. *See id.* at 26.
81. *Id.* at 36–37.
82. *Id.* at 38.
83. *Id.* at 36–37.
84. *Id.* at 38.
85. *Kapellas*, 1 Cal. 3d. at 37.
86. *Id.* at 38.
87. *See Diaz*, 139 Cal. App. 3d at 122–25.
88. *See id.* at 123.

and a local newspaper published a story on the controversy.[89] Somehow, a columnist discovered Diaz was transgender and publicized this fact, along with her legal name and ASAB.[90] Though the court admitted individuals who "voluntarily seek public office or willingly become involved in public affairs waive their right to privacy of matters connected with their public conduct," it found Diaz's gender identity was not newsworthy.[91] First, the court found the information lacked social value because there was no connection between Diaz's qualifications for office and her gender identity.[92] Although the question of whether the publication constituted a severe intrusion into Diaz's private life was a factual question for the jury, the court noted publications would not be privileged if they are so offensive that they constitute a "morbid and sensational prying into private lives for its own sake."[93] The court also found the question of whether Diaz voluntarily acceded to public notoriety was a factual question for the jury. However, it admitted the public arena Diaz entered was small, and being the first female student body president did not vindicate the disclosure—an indication the court did not find her transgender status central to the public's interest.[94] Also factoring into the court's decision, Diaz "scrupulously kept" her gender identity secret by changing her name and updating her driver's license, Social Security card, and high school records.[95]

However, *Diaz* does not signify a ban on all disclosures related to LGBTQIAP+[96] identities.[97] *Sipple v. Chronicle Publishing Co.* makes this clear. In *Sipple*, the California Court of Appeals found a public figure's sexual orientation constituted newsworthy information.[98] There, Oliver Sipple sued

89. *Id.* at 124.

90. *See id.*

91. *Id.* at 134.

92. *See id.* ("The fact that she is [transgender] does not adversely reflect on her honesty or judgment.").

93. *Diaz*, 139 Cal. App. 3d at 126 (quoting Virgil v. Time, Inc., 527 F.2d 1122 (9th Cir. 1975)). This insinuates the court's belief this publication constituted a severe intrusion into plaintiff's private life.

94. *See id.* at 134.

95. *Id.* at 123, 132.

96. The acronym LGBTQIAP+ stands for lesbian, gay, bisexual, transgender, queer, intersex, asexual, and pansexual/polysexual. The plus sign indicates any sexual or gender identities not captured by the acronym. Jesse Jade Turner, *LGBTQIAP+: We help you understand 23 gender terms*, PARENT24 (May 16, 2019), https://www.parent24.com/Teen_13-18/Development/lgbtqiap-we-help-you-understand-23-gender-terms-20190124 [https://perma.cc/8W5H-MCZ5].

97. The court in *Diaz* indicated Diaz's public disclosure claim was actionable not because the LGBTQIAP+ identity is necessarily private, but because she went to considerable lengths to maintain the confidentiality of her transgender identity. *But see Wasser*, 191 Cal. App. 3d at 1463 (distinguishing *Diaz*, where court dismissed plaintiff's invasion of privacy claim, where plaintiff brought suit against a newspaper for public disclosure for publishing a story on plaintiff being acquitted of murder, where the court held that unlike the plaintiff in *Diaz*, plaintiff here did not keep his acquittal secret but pursued various ancillary suits related to acquittal, thus vaulting himself into a place of public notoriety).

98. *See Sipple*, 154 Cal. App. 3d at 1048–50. This is not to say the lived experiences of transgender individuals and homosexual individuals are the same. They are not. Still, the California Court of Appeal's treatment of gender identity and sexual orientation serve as a useful point of comparison.

a newspaper for public disclosure of private facts for divulging his homosexuality in a news story.[99] After he foiled an assassination attempt on President Ford, Sipple garnered considerable publicity; subsequently, the San Francisco Chronicle published a story detailing how Sipple foiled the attempt, which would likely "break the stereotype" and instead influence the notion gay men were heroic.[100] The story was then run by the Los Angeles Times, then by various newspapers in other states.[101] Sipple sued, alleging he was not a public figure and his homosexuality was a private fact, as his family was unaware of his sexuality until the newspapers circulated it, which resulted in Sipple's family ostracizing him.[102] The court found Sipple's claim was not an actionable invasion of privacy.[103] It reasoned his homosexuality was not a "private" fact, as it was already widely known to the San Francisco community: the fact he frequented gay bars, marched in gay rights parades, and had a close public friendship with Harvey Milk (a prominent, openly gay man) meant his sexual orientation was public knowledge.[104] The court also emphasized that Sipple did not attempt to conceal his homosexuality. When asked, he would "frankly admit that he was gay."[105]

The *Sipple* court sidestepped the three newsworthiness factors, deciding the paramount test for newsworthiness was "whether the matter is of legitimate public interest which in turn must be determined according to the community mores."[106] The court found the newspaper's actions were not "morbid and sensational prying,"[107] but motivated by a legitimate interest in dismantling the stereotype that all gay men were "timid, weak, and unheroic" and raising the question of whether President Ford held prejudice against gay

99. *See id.* at 1043.
100. *See id.* at 1044.
101. *See id.* at 1043–44.
102. *See id.* at 1044–45, 1049.
103. *See Sipple*, 154 Cal. App. 3d at 1048.
104. *See id.*
105. *Id.* at 1048.
106. *Id.*
107. Interestingly, the California Court of Appeals did not cite to *Diaz*, in which it held just a year earlier disclosure of a public figure's transgender identity constituted a "morbid and sensational prying" into her private life. *Id.* at 1049. This possibly denotes the court was only willing to sanction disclosure of the LGBTQIAP+ identity in that specific case and would not broadly apply the *Diaz* holding in other similar circumstances. *Cf. Diaz*, 139 Cal. App. 3d at 126.

individuals, making the information newsworthy.[108] Finally, the court rejected Sipple's objection he was not a public figure because he did not intend to thrust himself into the limelight.[109] The court deemed Sipple an "involuntary public figure," saying there are some individuals who did not seek "publicity or [consent] to it, but through their own conduct or otherwise have become a legitimate subject of public interest. They have . . . become 'news' . . . These persons are regarded as properly subject to the public interest."[110] Thus, for the purposes of Sipple's public disclosure claim, he could be regarded as a public figure (albeit an involuntary one) and consequently the subject of legitimate public concern.[111]

Ultimately, public figures' ability to bring public disclosure claims is at the mercy of the newsworthiness determination, which is further complicated by the fact this determination is usually left to a jury's subjective judgment.[112] Compounding this is the role sensationalism plays in society's beliefs about what is newsworthy. To a large extent, sensationalism obfuscates the newsworthiness determination. Too often, trivial and lurid details of public figures' private lives are the subject of publicity.[113] This is to say, compared to private figures, public figures' ability to retain control over their private lives is flimsy.

C. The European Union's Right to Be Forgotten

The RTBF is an EU privacy right that grants citizens the ability to erase, limit, or delist personal data on the Internet which may be incorrect, embarrassing, irrelevant, or outdated.[114] The European Court of Justice (ECJ) first articulated the right in 2014 in *Google Spain SL v. Agencia Española de Proteción de Datos and Mario Costeja González* (*Google Spain*).[115] Upon Googling his name, Mario Costeja González discovered two links to a La

108. *Sipple*, 154 Cal. App. 3d at 1049. This exemplifies courts' belief that disclosure of sexual orientation is newsworthy if the disclosure is important to understanding the story being reported. This was discussed in Barbara Moretti's article, who explained sexual orientation is ordinarily a private fact, but media disclosure of sexual orientation will be privileged if it provides context to a news story. This notion undergirds the court's analysis in *Sipple*: it believed disclosure of Sipple's homosexuality constructed a heroic image, which contributed to an understanding of the assassination attempt. *See* Barbara Moretti, *Outing: Justifiable or Unwarranted Invasion of Privacy? The Private Facts Tort as a Remedy for Disclosures of Sexual Orientation*, 11 CARDOZO ARTS & ENT. L.J. 857, 896–97 (1993).

109. *See Sipple*, 154 Cal. App. 3d at 1049–50.

110. *Id.* at 1049–50 (quoting RESTATEMENT (SECOND) OF TORTS § 652D cmt. f).

111. *See id.* at 1050.

112. *See, e.g.*, *id.* at 1048.

113. Karcher, *supra* note 64, at 802 ("Much of today's news coverage . . . involves the publication of purely trivial information and events regarding public figures . . . including everything from child custody battles to failure to pay their debts. The publication of such trivial information does not serve the primary purpose of informing society. . . . ").

114. *See* Michael J. Kelly & David Satola, *The Right to Be Forgotten*, 2017 U. ILL. L. REV. 1, 3; Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 353 (2015).

115. *See Google Spain*, *supra* note 15.

Vanguardia article detailing an auction to pay off social security debts, which González claimed he repaid.[116] González requested La Vanguardia either remove or change the webpages so that Google searches of his name would no longer reveal this personal data.[117] He also asked the court to order Google Spain or Google Inc. to remove his personal data so the article would no longer appear and so his name would not be visible in links to the article.[118] González contended any articles detailing the attachment proceeding were no longer relevant, as he had paid the debts years ago.[119] In responding to González's complaint, the ECJ determined whether the right to privacy furnished by the EU's Data Protection Directive (the Directive) protected the *processing* of González's personal data, thus obliging Google to remove González's name from searches conducted for his name.[120] The ECJ ruled in González's favor, finding the Directive required Google to delist links to the La Vanguardia article.[121]

In doing so, the ECJ enunciated the standard for invoking the RTBF: a data subject can compel a data controller[122] to delist information if it is inadequate, irrelevant, or excessive in relation to the purposes for which they are collected.[123] In articulating this standard, the ECJ noted a data subject can still request a controller to delist information even if the information is true and "published lawfully by third parties," so long as it does not comply with the criteria set out by Article 6 of the Directive.[124]

The ECJ's decision also had some significant qualifications. One of the significant caveats was the "journalistic purposes" exception, which exempted third-party publishers from delisting obligations for information

116. *See id.* ¶ 14.
117. *See id.* ¶ 15.
118. *See id.*
119. *See id.*
120. *See id.* ¶¶ 1–3.
121. *See Google Spain*, *supra* note 15, ¶ 98.
122. A data controller is any "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) art. 2(d), https://eur-lex.europa.eu/eli/dir/1995/46/oj [hereinafter, *Directive 1995/46/EC*]. Here, the ECJ considered Google—and notably, not La Vanguardia—to be a data controller, as Google dictated the processing of González's personal data online by "loading [his] data on an Internet page." *Google Spain*, *supra* note 15, ¶ 35. In contrast, the court determined La Vanguardia was an online publisher of the underlying article at issue and as such did not engage in the same processing actions as Google.
123. *See Google Spain*, *supra* note 15, ¶ 72.
124. *See id.* ¶ 85. Article 6 reads in relevant part: "Member States shall provide that personal data must be: processed fairly and lawfully . . . collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes . . . adequate, relevant and not excessive in relation to the purposes for which they are collected . . . accurate and, where necessary, kept up to date. . . . " *Directive 1995/46/EC*, *supra* note 122, art. 6.

published for "journalistic purposes."[125] In compelling Google to delist links to the La Vanguardia article, the ECJ distinguished between Google's actions as a data controller that processed personal data and La Vanguardia's actions as an online publisher.[126] The ECJ said La Vanguardia's actions of publishing personal information in online articles does not constitute "processing of personal data" by a data controller like Google within the meaning of the Directive.[127] Thus, La Vanguardia's actions as a third-party publisher were not tantamount to those of Google as a data controller.[128] To that end, the ECJ exempted third-party publishers from delisting obligations so long as they published a data subject's personal information exclusively for "journalistic purposes"[129] under Article 9.[130] This means it is possible for data subjects to have a claim against data controllers, but not against online publishers. The ECJ held La Vanguardia printed González's personal information for journalistic reasons, meaning that the RTBF imposed delisting obligations on Google, but not on La Vanguardia, thus freeing the newspaper from an obligation to delete the article.[131]

Though the ECJ limited its holding by not imposing any delisting obligations on La Vanguardia, many lower European courts have skirted the "journalistic purposes" exception and imposed delisting and sometimes even deletion obligations on publishers directly. This is the subject of the following section.

Despite the ECJ's efforts to cabin the RTBF's delisting obligations to data controllers alone, many lower European courts have imposed erasure obligations on both data controllers and publishers of online articles alike. Lower courts' treatment of publishers varies.[132] Some mandate that third-party publishers delist online articles and anonymize them by redacting a data

125. *See Google Spain*, *supra* note 15, ¶ 85.

126. *See id.* ¶ 35.

127. *See id.*

128. *See id.*

129. Article 9 also exempts publishers from delisting obligations if they publish a data subject's personal information exclusively for "expressive" purposes. *See Directive 1995/46/EC*, *supra* note 122, art. 9 ("Member States shall provide for exemptions . . . for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.").

130. *See Google Spain*, *supra* note 15, ¶ 85.

131. *See id.*

132. *See* S.T.S., Oct. 15, 2015 (J.T.S. No. 545/2015) (Spain), http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7494889&links=%222772%2F2013%22%20%22545%2F2015%22&optimize=20151019&publicinterface=true [https://perma.cc/75CS-GKWY] (Spanish Supreme Court interpreting the RTBF to impose delisting obligations on online publishers); Hof van Cassatie [Cass.] [Court of Cassation], 29 Apr. 2016, AR C150052F, http://www.cass.be (Belg.), https://inforrm.files.wordpress.com/2016/07/ph-v-og.pdf [https://perma.cc/326M-8AN2] (Belgian Court of Cassation construing the RTBF to require a publisher to delist and anonymize an online article); Cass., sez. un., 24 giugno 2016, n. 13161, Giur. it. 2016, II, 1 (It.), http://www.altalex.com/documents/news/2016/07/07/cronaca-e-diritto-all-oblio [https://perma.cc/84X8-8295] (Italian Supreme Court of Cassation interpreted RTBF to necessitate a publisher's deletion of a true two-year old online article).

subject's personal information while others have gone so far as to require third-party publishers to delete entire articles from the Internet. In her 2018 article, Professor Dawn C. Nunziato detailed how lower courts have expanded the RTBF by imposing erasure and anonymization obligations on third-party publishers of online content, arguing that lower courts have "upset the balance that the [ECJ] initially carefully established between data subjects' privacy rights and newspapers' right to freedom of expression and journalistic privileges."[133]

The Spanish Supreme Court further expanded the RTBF by imposing delisting obligations on publishers of online articles in *A & B v. Ediciones El País SL*.[134] There, two former drug traffickers sued El País, a Spanish newspaper, for indexing online articles detailing their convictions.[135] The men argued that because the offenses occurred years ago and they were now rehabilitated working professionals, the article was irrelevant and should be made inaccessible.[136] The court rejected El País's argument that the journalistic purposes exception shielded it from liability and said the delisting obligations imposed on data controllers by the RTBF included not only search engines, but also third-party publishers of online content acting as data controllers.[137] The court held El País's processing of the men's personal data was no longer "adequate, relevant, and not excessive," asserting the press's primary purpose is to report on current events, with the archiving of past news being secondary.[138] The court determined that enough time had passed such that continued processing of this information was unnecessary and thus that the plaintiffs' privacy rights outweighed El País's expressive freedoms.[139] As such, the court ordered El País to hide the article from the public by making it inaccessible via general searches.[140]

The Belgian Court of Cassation expanded the RTBF further by imposing both delisting and anonymizing obligations on a publisher in *Olivier G v. Le Soir*.[141] There, Olivier G sued a newspaper for processing an online

133. Nunziato, *supra* note 15, at 1031.

134. *See* S.T.S., Oct. 15, 2015 (J.T.S. No. 545/2015) (Spain), http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7494889&links=%222772%2F2013%22%20%22545%2F2015%22&optimize=20151019&publicinterface=true [https://perma.cc/75CS-GKWY].

135. *See* Nunziato, *supra* note 15, at 1022 (summarizing S.T.S., Oct. 15, 2015 (J.T.S. No. 545/2015) (Spain)).

136. *See id.* at 1022–23 (summarizing S.T.S., Oct. 15, 2015 (J.T.S. No. 545/2015) (Spain)).

137. *See id.* at 1023 (summarizing S.T.S., Oct. 15, 2015 (J.T.S. No. 545/2015) (Spain)).

138. *Id.* at 1023–24 (explaining S.T.S., Oct. 15, 2015 (J.T.S. No. 545/2015) (Spain)).

139. *Id.* at 1024 (explaining S.T.S., Oct. 15, 2015 (J.T.S. No. 545/2015) (Spain)).

140. *Id.*

141. Nunziato, *supra* note 15, at 1027–28 (summarizing Hof van Cassatie [Cass.] [Court of Cassation], 29 April 2016, AR C150052F, http://www.cass.be (Belg.), https://inforrm.files.wordpress.com/2016/07/ph-v-og.pdf [https://perma.cc/326M-8AN2]).

article detailing a fatal accident he caused by driving while intoxicated.[142] Upon discovering the article, Olivier G requested the newspaper anonymize it by replacing his name with an "X", but the newspaper refused, so he sued, claiming the newspaper's refusal contravened the RTBF.[143] Over the newspaper's objections that the journalistic purposes exception protected its actions, the court ruled in Olivier G's favor.[144] The court held that the RTBF enables individuals with past convictions to object to the availability of their criminal histories online, and that Olivier G's privacy interests superseded the newspaper's expressive freedoms because the availability of his criminal past online did more harm to him than it did to promote press freedoms.[145]

On the most extreme end of the spectrum is the Italian Supreme Court of Cassation.[146] The court extended RTBF obligations to PrimaDaNoi, an Italian newspaper publisher, requiring them to delete an article that it published two years prior.[147] At issue was an article published by an Italian newspaper, PrimaDaNoi, detailing assault charges brought against a restaurant owner.[148] Just two years after the article's publication, the restaurant owner, believing the online article marred his and his restaurant's reputation, demanded PrimaDaNoi delete it.[149] PrimaDaNoi refused.[150] The Court rejected PrimaDaNoi's argument that it was shielded by the journalistic purposes exception, finding the article was more harmful to the restaurant owner's privacy rights than it was beneficial to PrimaDaNoi's expressive freedoms despite the fact that the article was only two years old and that the criminal suit was ongoing.[151] The court determined the public's interest in the criminal proceedings against the restaurant owner was satisfied because the article was available online for two years. In the court's view, the public's interest in the information elapsed since its publishing, and thus the proper remedy was deleting the article.[152]

These European lower court decisions expanded the RTBF by holding privacy rights supersede the media's press and expressive freedoms. Many

142. *See id.*

143. *See id.*

144. *See id.* at 1028.

145. *See* Aaron Minc, *Right to Be Forgotten Requires Anonymization of Online Newspaper Article*, MINC L. (Sept. 14, 2018), https://www.minclaw.com/right-to-be-forgotten-requires-anonymisation-online-newspaper-article/ [https://perma.cc/ZLS4-DVYF] (summarizing the Belgian Court of Cassation's holding in Olivier G v. Le Soir).

146. Cass., sez. un., 24 giugno 2016, n. 13161, Giur. it. 2016, II, 1 (It.).

147. Nunziato, *supra* note 15, at 1029 (summarizing Cass., sez. un., 24 giugno 2016, n. 13161, Giur. it. 2016, II, 1 (It.)).

148. *See* Adam Satariano & Emma Bubola, *One Brother Stabbed the Other. The Journalist Who Wrote About It Paid a Price*, N.Y. TIMES (Sept. 23, 2019), https://www.nytimes.com/2019/09/23/technology/right-to-be-forgotten-law-europe.html [https://perma.cc/KAG2-FU2Q].

149. *See* Nunziato, *supra* note 15, at 1030 (summarizing Cass., sez. un., 24 giugno 2016, n. 13161, Giur. it. 2016, II, 1 (It.)). *See also* Satariano & Bubola, *supra* note 148.

150. *See id.*

151. *See id.* (summarizing Cass., sez. un., 24 giugno 2016, n. 13161, Giur. it. 2016, II, 1 (It.)).

152. *See id.*

believe the legal theories undergirding these decisions represent a stark departure from the U.S.'s concept of privacy.[153] The following section details how the RTBF would clash with American First Amendment freedoms, and how that tension can be resolved to allow transgender public figures to retain control over their personal information.

III. PROTECTING TRANSGENDER PUBLIC FIGURES' PRIVACY RIGHTS WITH THE RTBF

A. Privacy Law: No Recourse for Transgender Public Figures

The balancing act courts conduct when analyzing a public disclosure claim raises distinct concerns with respect to transgender individuals. Though transgender persons' needs to maintain the confidentiality of their personal information to actualize their true gender identity is a weighty privacy interest, courts may not honor this interest, especially if a transgender person is a public figure and a court finds publication of their personal information necessary to satiate a legitimate public interest.[154] While it is true the First District of the California Courts of Appeal in *Diaz v. Oakland Tribune* enabled a transgender public figure to sue a newspaper for public disclosure for publishing her legal name and ASAB, this should not be read as an outright ban on the disclosure of a transgender public figures' gender identity.[155] There are a few reasons this decision is insufficient to resolve this issue.

First, *Diaz* was a state court decision, so it is not binding on other jurisdictions.[156] Second, the court's decision was cabined to its facts. The court was careful to indicate Diaz's public disclosure claim was actionable because she took extensive measures to keep her gender identity secret.[157] This suggests the court would be unwilling to penalize disclosure of a transgender public figure's gender identity if they did not "scrupulously [keep it] a secret."[158] Moreover, while the court agreed she was a public figure, it explained that the public arena for a university's student body president is small,[159] which suggests a transgender public figure with greater notoriety than Diaz, such as an actress or senator, may not rely on this decision. Third, it is significant the court decided this case in 1983, when the modern Internet

153. *See id.* at 1042.

154. *Id.*

155. *See Diaz*, 139 Cal. App. 3d 118.

156. It does not even seem to be binding in its own jurisdiction, as the California Court of Appeals did not cite to *Diaz* in a holding articulated one year later in *Sipple v. Chronicle Publishing Co. See Sipple*, 154 Cal. App. 3d 1040. Though *Diaz* involved disclosure of a plaintiff's transgender status and *Sipple* involved disclosure of a plaintiff's homosexuality, the issues are closely related as they both involve disclosures concerning LGBTQIAP+ identities.

157. *See Diaz*, 139 Cal. App. at 132.

158. *Id.* at 123.

159. *Id.* at 134.

did not exist.[160] Today, individuals often use the Internet in a way that compromises their privacy,[161] necessarily making it more difficult to guard against unwanted disclosures, a reality that courts must respond to when assessing individuals' information privacy rights today.[162] Also, were the same facts litigated today, a court could easily decide the other way, given the prevalence of anti-transgender policies implemented under President Trump's Administration,[163] and especially given Trump's appointment of numerous conservative justices with records of opposing LGBT+ rights to the federal bench.[164] Thus, it is unlikely a transgender public figure would be able to rely

160. One could argue that the fact that *Diaz* was decided in 1983 cuts in the other direction because, in theory, society's perception of transgender individuals has improved since then. However, given the rampant violence perpetuated against transgender individuals today, this is not an ironclad argument. *See, e.g.*, James et al., *supra* note 17; *Fatal Violence Against Transgender People in America 2017*, *supra* note 24; Fadulu, *supra* note 17 and accompanying text.

161. *See* Thomas H. Koenig & Michael L. Rustad, *Digital Scarlet Letters: Social Media Stigmatization of the Poor and What Can Be Done*, 93 NEB. L. REV. 592, 595 (2015).

162. *See* Agnieszka A. McPeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 WAKE FOREST L. REV. 887, 946 (2013).

163. *See* Fadulu, *supra* note 17. *See also* Lee *supra* note 28, at 1415.

164. *See, e.g.*, *On the Bench: Federal Judiciary*, AM. CONST. SOC'Y (Dec. 18, 2020) https://www.acslaw.org/judicial-nominations/on-the-bench/ [https://perma.cc/T9U3-A6WA] (President Trump has confirmed 233 Article III judges to the federal bench during his administration, including three Supreme Court Justices); Colby Itkowitz, *1 in Every 4 Circuit Court Judges is Now a Trump Appointee*, WASH. POST (Dec. 21, 2019, 7:32 PM), https://www.washingtonpost.com/politics/one-in-every-four-circuit-court-judges-is-now-a-trump-appointee/2019/12/21/d6fa1e98-2336-11ea-bed5-880264cc91a9_story.html [https://perma.cc/V97Z-H9WN] (noting that Trump's aggressive installment of federal judges "has remade the federal judiciary, ensuring a conservative tilt for decades and cementing his legacy. . . . "); *Trump's Judicial Assault on LGBT Protections*, LAMBDA LEGAL 7–8 (2019), https://www.lambdalegal.org/sites/default/files/publications/downloads/trump-judicial-nominees-report-2019.pdf [https://perma.cc/XDL5-4UG8] (citing Gibson v. Collier, 920 F.3d 212 (5th Cir. 2019)) (observing that "over-one third of Trump's judicial nominees to the circuit courts have[] records of working to undermine LGBT rights and protections", noting the discriminatory conduct of Trump-appointee Judge James Ho, who sits on the U.S. Court of Appeals for the Fifth Circuit. Judge Ho authored an opinion in which he denied a transgender female inmate healthcare and continuously misgendered her "by using improper pronouns throughout the decision, even after the district court had used the correct pronouns."). *See also Gibson*, 920 F.3d at 216–17 (Judge Ho mentioned that Gibson was a transgender woman and that she "lived as a female since the age of 15" and used the name "Vanessa Lynn Gibson," but referred to her using male pronouns and her deadname, "Scott Lynn Gibson," throughout the decision).

on *Diaz* to assert their informational privacy rights and adequately protect themselves from discrimination.[165]

Even when courts find public disclosure claims actionable, the remedies available are inadequate to fully rectify the harm done to transgender individuals by the disclosure of their personal information. If a court finds a public figure's public disclosure claim actionable, it will either award the plaintiff damages or order an injunction to restrain further publication of the information at issue.[166] For example, in *Diaz*, the court upheld the jury's award of $250,000 in compensatory damages and $525,000 in punitive damages,[167] which the court said was meant to reflect the visceral pain Diaz suffered, but conceded the harm done to her by the newspaper revealing her ASAB and birth name was "not easily quantifiable."[168] To the court's point, monetary damages cannot fully compensate a transgender person for being "outed." Money cannot resolve the fact a publication has invalidated a transgender person's gender identity by bringing to the forefront of the public's mind their former identity, essentially undermining all of the work they undertook to transition.[169] Money also cannot compensate for the stigma[170] and physical violence[171] to which disclosure of this information exposes them. Nor can an injunction fully resolve the issue, because while a court can enjoin a newspaper from publicizing this information further, once it has been published, there is no way to erase this information from the public domain.[172]

To fully resolve this issue and ensure transgender public figures retain control over their personal information such that it does not pose a threat to their safety or inhibit them from expressing their gender identity requires looking across the Atlantic towards the EU's RTBF. The following section details how the U.S. might fashion a similar privacy right modeled after the RTBF. Importantly, the subsequent section does not recommend a verbatim importation of the *Google Spain* decision. Rather, it proposes forging a privacy right for transgender public figures based on the lower European

---

165. Another important point to consider is the degree to which public figures use the Internet and social media today. Many celebrities and politicians use social media to make announcements, garner notoriety, and connect with the public. *See* Sherilynn Macale, *Why More Celebrities and Public Figures Are Turning to Social Media*, THE NEXT WEB (Oct. 17, 2011), https://thenextweb.com/socialmedia/2011/10/17/why-more-celebrities-and-public-figures-are-turning-to-social-media/ [https://perma.cc/P32Y-9MEY]; *see also* Jennifer Goldbeck et al., *Twitter Use by the U.S. Congress*, 61 J. AM. SOC'Y INFO. SCI. TECH. 1612 (2010) (exploring congresspersons' Twitter usage to self-promote and disseminate information to their constituents about their daily activities).

166. 4 TEXAS TORTS AND REMEDIES, *supra* note 36.

167. *See Diaz*, 139 Cal. App. 3d at 122.

168. *See id.* at 137.

169. SHULTZ, *supra* note 18, at 200–01.

170. Rainey & Isme, *supra* note 27 and accompanying text.

171. *See* Lee, *supra* note 28, at 1415 and accompanying text.

172. *See Garcia*, 786 F.3d at 745 (stating there is no RTBF in the U.S.).

courts' expansion and application of the RTBF. This is because simply delisting articles that reference transgender public figures' birth name and ASAB does not completely remedy the harm done by revelation of such information. The way to fully remedy such harm is by requiring the delisting of online articles that reference such information, as well as redacting such information from the online articles themselves.

B. Implementing the RTBF: How Feasible is an American Right of Erasure?

Before delving into how the U.S. may adopt the RTBF, it merits contextualizing American opposition to it. As the Ninth Circuit explained in *Garcia v. Google*, there is decidedly no RTBF in the U.S.[173] The unwillingness to recognize the RTBF stems from the belief it is anathema to First Amendment speech and press freedoms.[174] This is due to the power conferred by the RTBF because it is perhaps the greatest informational privacy mechanism ever, as it creates a right to wipe from the Internet any information a person deems unfavorable.[175] In this respect, the RTBF conflicts with Americans' guaranteed speech and press freedoms because the removal of information from online publications necessarily occludes the press's freedom to publish it.[176] There is also a concern the RTBF would signal the end of a free and open Internet, which is integral to the uninhibited expression of speech and exchange of information.[177]

However, there is reason to doubt legal scholars' and practitioners' concerns that the RTBF is incompatible with American legal principles. In fact, there are several aspects of American law that embrace the essence of the RTBF[178]—that is, the belief that some information is so private it should be redacted from the public sphere. For example, criminal erasure statutes that expunge a person's criminal records create a "legal fiction" that that person

---

173. *Id.*

174. *See* Editorial, *Ordering Google to Forget*, N.Y. TIMES (May 13, 2014), https://www.nytimes.com/2014/05/14/opinion/ordering-google-to-forget.html?hp&rref=opinion [https://perma.cc/97JF-W353].

175. *See generally* Eric Posner, *We All Have the Right to Be Forgotten*, SLATE (May 14, 2014), https://slate.com/news-and-politics/2014/05/the-european-right-to-be-forgotten-is-just-what-the-internet-needs.html [https://perma.cc/AZF5-M8YL].

176. Editorial, *supra* note 174 ("Lawmakers should not create a [RTBF] so powerful that it could limit press freedoms or allow individuals to demand that lawful information in a news archive be hidden.").

177. *See* Jeffery Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (Feb. 13, 2012), https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf [https://perma.cc/PC7Q-JTNC] ("Unless the [RTBF] is defined more precisely . . . it could precipitate a dramatic clash between European and American conceptions of the proper balance between privacy and free speech, leading to a far less open Internet.").

178. *See* Amy Gajda, *Privacy, Press, and the Right to be Forgotten in the United States*, 93 WASH. L. REV. 201, 206 ("[T]he essential elements of a Right to Be Forgotten have been a part of both U.S. common law and statutory law for decades, in spite of constitutional protections for the publication of truthful information.").

was never convicted.[179] This principle is also exemplified in the Restatement of Torts when it references the sort of private facts that give rise to actionable public disclosure claims, acknowledging there are parts of "[one's] past that he would rather forget."[180]

Further cementing feasibility of implementing the RTBF is the changed circumstances surrounding privacy law, evidenced by the increased demand for an American RTBF in recent years. Jurisprudence is often remade by social changes surrounding the law.[181] One significant social change since Warren's and Brandeis' article 130 years ago is the permanence of information, thanks to the Internet. The Internet's indelible recording of personal information is the reason people today must "live with the digital baggage of their pasts."[182] Such digital permanence has engendered a demand for a RTBF-type mechanism; this can be seen through the existence of certain legal mechanisms that emulate the RTBF's essential function.[183] One such mechanism is copyright law—specifically, the Digital Millennium Copyright Act (DMCA)'s takedown notice.[184] A takedown notice is a written request from a copyright owner to an Internet service provider (ISP) in which the copyright owner claims their copyrighted material is being infringed upon and requests the ISP remove the material from the Internet.[185] *Garcia v. Google*

179. Martin v. Hearst Corp., 777 F.3d 546, 550 (2d Cir. 2015).

180. *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. b.

181. Lynton Keith Caldwell, *Land and the Law: Problems in Legal Philosophy*, U. ILL. L. REV. 319, 320 (1986) (explaining land law reflects "prevailing social attitudes," and "when social attitudes change, the law will follow sooner or later.").

182. Daniel J. Solove, *Speech, Privacy, and Reputation on the Internet*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 15, 18 (Saul Levmore et al. ed., 2012).

183. For example, this section discusses the Takedown Notice of the Digital Millennium Copyright Act (DMCA), which grants a copyright owner a legal mechanism to request their copyrighted material be removed from the Internet if such material is infringed upon—imitating the RTBF's delisting function. *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 and 28 U.S.C.) [hereinafter, Digital Millennium Copyright Act]. There is also existing research that outlines the demand for an American RTBF, much of which focuses on the way existing American legal structures already embrace the RTBF. *See, e.g.*, Edward J. George, *The Pursuit of Happiness in the Digital Age: Using Bankruptcy and Copyright Law as a Blueprint for Implementing the Right to Be Forgotten in the U.S.*, 106 GEO. L. J. 905, 928 (2018) (asserting that the digital permanence guaranteed by the Internet creates an impetus to import the RTBF, and moreover that the RTBF already exists in American legal mechanisms, such as the Takedown Notice of the DMCA, which requires the removal of certain webpages that infringe upon copyrighted materials); Brian O'Shea, *A New Method to Address Cyberbullying in the United States: The Application of a Notice-and-Takedown Model as a Restriction on Cyberbullying Speech*, 69 GEO. WASH. FED. COMM. L. J. 119, 121–23 (2017) (observing the impetus for an American RTBF to curb the alarmingly permanent impact of cyberbullying, finding that "there already exists a comparable mechanism" in the form of the DMCA's Takedown Notice).

184. *See* 112 Stat. 2860.

185. *See, e.g.*, 17 U.S.C. § 512(c); Andre Menko Bleech, *What's the Use? Good Faith Evaluations of 'Fair Use' and Digital Millennium Copyright Act 'Takedown' Notices*, 18 COMMLAW CONSPECTUS 241, 243 (2009).

denotes the parallels between the DMCA's takedown notice and the RTBF's erasure mechanism. In *Garcia*, Garcia played a role in a film that, unbeknownst to her, was later turned into an Islamophobic film and uploaded to the Internet.[186] After experiencing considerable social backlash for her role, Garcia sent Google five takedown notices to remove the video from the Internet, asserting that the film's online presence violated her copyright interest in her performance.[187] Google refused, so she sued.[188] Though the Ninth Circuit found Garcia's copyright claim too weak and denied her request to remove the video—affirming that no RTBF exists in the U.S.—*Garcia* stands for more than just a single American court's refusal to recognize the RTBF.[189] Rather, it signifies efforts to carve a RTBF out of existing law. These examples substantiate that there is a developing desire for such a mechanism in the U.S., and also the potential that a RTBF could descend naturally from existing law.

The above indicates that a solution modeled after the RTBF to protect transgender public figures' privacy rights would not be so foreign as to make American application of this right completely infeasible, which the subsequent section outlines in greater detail.

Resolving this issue requires implementing the RTBF to create a right specific to transgender public figures—one that would enable them to erase their private information, if unveiled, from the public's view. Doing so requires going further than the ECJ did in *Google Spain*. As explained above, the ECJ's decision in *Google Spain* mandated only that data controllers—like Google and other search engines—were required to delist articles resulting from a search of a data subject's name.[190] Importing the *Google Spain* decision is insufficient because requiring the delisting of articles that reference transgender public figures' birth names and ASAB does not fully capture the harm done to these individuals. Instead, the U.S. should import the lower European courts' application of the RTBF. The Spanish Supreme Court, Belgian Court of Cassation, and Italian Court of Cassation are instructive inasmuch as they bookend how far the U.S. should go in adopting a RTBF to protect the privacy rights of transgender public figures.

However, the U.S. should borrow from the Spanish and Belgian courts, but not from the Italian Court. The Italian court's decision to order the deletion of an article that was true and relatively recent at the time of the decision was too far-reaching, and in recommending a solution, it is important to be realistic about what will comport with First Amendment freedoms in the U.S. Complete deletion of online articles so radically contravenes speech and press freedoms that it would make implementation untenable. The U.S. should follow the Spanish Supreme Court instead by imposing delisting

186. *See Garcia*, 786 F.3d at 737–38.
187. *See id.* at 738.
188. *See id.*
189. *Id.* at 745–46.
190. *See Google Spain*, *supra* note 15, ¶¶ 82, 88.

obligations on both data controllers and third-party publishers of online articles referencing transgender public figures' personal information.

The U.S. should also emulate the Belgian Court of Cassation. Upon receiving requests from transgender public figures to delist articles, the U.S. should order anonymization of the article by requiring third-party publishers to redact transgender public figures' personal information from the articles. In practice, this anonymization would come in the form of replacing transgender public figures' ASAB and legal names with an "X."[191] The U.S. should also subject both data collectors and publishers to liability if they refuse to honor the requests of transgender public figures to delist articles and redact their personal information.

The next question is what this solution will look like. Given that privacy law in the U.S. varies by state, it would be best for Congress to pass comprehensive federal legislation as opposed to relying on the Supreme Court to solve the problem. This would both eliminate jurisdictional variation and circumvent the Court's obligation to overturn a vast amount of precedent to create such a right. That said, it is not this Note's objective to supply the exact blueprint of this legislation; that is a task ripe for further discussion and research by another author. This Note's purpose is solely to assert that transgender public figures' privacy rights merit protection and to identify the RTBF as a mechanism to do so.

IV. CONCLUSION

The tenuous ability of public figures to assert their information privacy rights is qualified by the value of their actions to the public. This presents a quandary for transgender public figures, whose needs to maintain the confidentiality of their ASAB and legal names are essential to actualizing their gender identities. Even if transgender public figures are permitted to recover, such legal remedies are insufficient to fully ameliorate the harm done to them by disclosure. Without a right of erasure to delete this information from the public domain, transgender public figures are vulnerable to further discrimination and stigmatization, which is why the RTBF is essential to resolving this issue.

When envisioning how legal structures oppress transgender individuals, privacy law is not the first thing that comes to most people's minds. However, the legal issue this Note seeks to resolve typifies one of the ways those with the power to do so can reform privacy law to support transgender individuals and other minority groups. A classic example of how privacy law has been used to support minority groups is *Lawrence v. Texas*.

191. Much like the "X" Olivier G requested the Belgian newspaper replace his personally identifying information with in *Olivier G v. Le Soir*. *See* Nunziato, *supra* note 15, at 1027 (summarizing Hof van Cassatie [Cass.] [Court of Cassation], 29 April 2016, AR C150052F, http://www.cass.be (Belg.)).

There, the Supreme Court used privacy jurisprudence to protect the rights of LGBTQ+ persons to engage in consensual sexual intercourse in the privacy of their own homes.[192] This issue similarly is another way privacy law can be used to support the needs of another marginalized community. This solution may seem extreme to those who strongly favor First Amendment freedoms, but what is more extreme is the violence and prejudice transgender individuals still face—and rectifying this issue is essential to uplifting transgender individuals and protecting them from discrimination.

192. Lawrence v. Texas, 539 U.S. 558, 578 (2003).

In Antitrust We Trust?: Big Tech Is Not the Problem—It's Weak Data Privacy Protections

Olivia T. Creser*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School; B.F.A., Photography, Parsons, The New School. I would like to thank the staff of the Federal Communications Law Journal for their patience and assistance in bringing this Note to publication.

I. INTRODUCTION

The Big Tech companies—Amazon, Apple, Facebook, and Google[1]—which many once admired as the trailblazers that brought the technology frontier to America's front door, have fallen out of favor with a public that no longer trusts how important these firms are to American life.[2] The idea to break up Big Tech has been around for over a decade,[3] but the movement did not become mainstream until 2019 when Democratic presidential candidates were asked to debate the topic for the first time on a national stage, exposing the shift in public opinion.[4]

That same year, some of Big Tech's most notable pioneers turned their backs on the companies they helped to start. Apple co-founder Steve Wozniak said in an interview he "wish[es] Apple on its own had split up a long time ago," and thought that Big Tech has "taken our choices away."[5] Facebook co-founder Chris Hughes echoed these sentiments in a *New York Times* opinion column where he mused about his own use of Facebook, saying, "The choice is mine, but it doesn't feel like a choice."[6] Hughes joined the call to break up Facebook, attributing the platform's privacy missteps to its quest for "domination."[7]

The shift in attitude toward Big Tech runs parallel to a movement fervently working to chip away at the edifice of antitrust doctrines that have dominated jurisprudence since the 1970s.[8] This group, referred to as the New Brandeis School,[9] is not only motivated by the power of Big Tech but also

---

1. Microsoft is often included in this grouping.

2. Theodore Schleifer, *Why Does Washington Suddenly Seem Ready to Regulate Big Tech? Look at the Polls*, VOX MEDIA (June 4, 2019), https://www.vox.com/2019/6/4/18652469/washington-antitrust-regulate-amazon-google-facebook-look-at-polls [https://perma.cc/QB3J-CXVG] (citing a 2019 Harris Poll that showed the reputations of Google and Facebook dropped 13 and 43 slots respectively among how Americans view them).

3. *See* Tim Wu, *In the Grip of the New Monopolists*, WALL ST. J. (Nov. 13, 2010, 12:01 AM), https://www.wsj.com/articles/SB10001424052748704635704575604993311538482 [https://perma.cc/8PUW-YZTC].

4. Emily Birnbaum, *Democrats Wrangle Over Whether to Break Up Big Tech in Debate First*, THE HILL (Oct. 15, 2019), https://thehill.com/policy/technology/466008-democrats-wrangle-over-whether-to-break-up-big-tech-in-debate-first [https://perma.cc/VYC4-QZR4] (comparing candidates' views to those of Republicans and Democrats during the 2016 election wherein both parties "sought to court companies like Facebook and Google").

5. Mikey Campbell, *Steve Wozniak Says Apple Should Have Split Up Long Ago, Talks Push into Services and More*, APPLE INSIDER (Aug. 27, 2019), https://appleinsider.com/articles/19/08/27/steve-wozniak-says-apple-should-have-split-up-long-ago-talks-push-into-services-and-more [https://perma.cc/28FL-DEBB].

6. Chris Hughes, Opinion, *It's Time to Break Up Facebook*, N.Y. TIMES (May 9, 2019), https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html [https://perma.cc/9QX2-8LGJ].

7. *Id.*

8. *See infra* Section III.B.

9. The group has also been referred to as the Hipster Antitrust Movement. *See* Andrea O'Sullivan, *What Is 'Hipster Antitrust?'*, MERCATUS CTR.: THE BRIDGE (Oct. 18, 2018), https://www.mercatus.org/bridge/commentary/what-hipster-antitrust [https://perma.cc/9GTV-URCB].

sees consolidation across a number of industries as a sign that antitrust law is failing to curb excessive accumulations of power.[10] The New Brandeis School is pushing to activate antitrust law against a number of social, economic, and political ills associated with the power of Big Tech and consolidation of power generally.[11] This Note focuses on particular ills that some have identified as symptomatic of Big Tech—namely, consumer exploitation, manipulation, and data privacy violations.[12]

The New Brandeisians have identified the size of Big Tech as the source of consumer harm online. However, these harms are symptoms of one of the basic principles that created the Internet ecosystem as we know it today, that is, the unregulated collection of consumer data for commercial purposes. This principle enables practices that exploit, manipulate, and violate the privacy of consumers to grow and persist. Therefore, breaking up Big Tech will not stop these harms from continuing to occur. Instead of focusing on Big Tech, this Note proposes that Congress and regulators prioritize the true cause of consumer exploitation, manipulation, and privacy violations—weak data privacy protections.

Section II of this Note explains the evolution of the Internet ecosystem and identifies the characteristics of Big Tech firms. In addition, it refutes arguments claiming that Big Tech's dominance is the cause of consumer exploitation, manipulation, and privacy violations in the digital marketplace with examples of consumer harm persisting throughout the Internet ecosystem. Section III discusses the inadequacies of the New Brandeisian approach to the power of Big Tech. Section IV shows that a strategy to curb consumer harm online that focuses on the power of Big Tech will fail to make a sufficient impact. Section V proposes a solution to consumer harm online that rests in a modification to the FTC's Section 5 authority, which will enable the agency to enforce data privacy protections that a reasonable consumer will expect.

II. BACKGROUND

A. The Internet's Move to a Centralized Ecosystem

The Internet ecosystem is defined as an "internet-dependent . . . business-enabling system within the broader economy, defined by activities that rely on the internet to promote exchanges of products, services, and information."[13] Since its humble beginning in the early 1990s, the modern

10. *See generally* TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE (2018).

11. *Id.*

12. *See e.g.*, Hughes, *supra* note 6; *see* Matt Stoller, Opinion, *Tech Companies Are Destroying Democracy and the Free Press*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/tech-monopoly-democracy-journalism.html [https://perma.cc/HB8V-MZPY]. These harms are not an exhaustive list of harms associated with the power of Big Tech.

13. JOHN DEIGHTON ET AL., INTERACTIVE ADVERTISING BUREAU, ECONOMIC VALUE OF THE ADVERTISING-SUPPORTED INTERNET ECOSYSTEM 115 (2017).

Internet has grown exponentially from 3,000 websites in 1994 to 1.72 billion websites today.[14]

Contrary to the increase in the number of websites, actual page views have decreased over time. "While in 2001, the top 10 websites accounted for 31 percent of all page views in America, by 2010 the top 10 accounted for 75 percent."[15] This paradox defies initial projections about the decentralized nature of the Internet.[16]

Tim Wu, a leading New Brandeisian, when asked in an interview in 2010 whether he thought the technology monopolies of that time looked different than those of the past, he replied, "I know the Internet . . . was designed to resist centralized control . . . [b]ut firms today, like Apple, make it unclear if the Internet is something lasting. . . ."[17] At that time, companies like Apple and Google began to dominate their respective markets.[18] Even then, many believed that the Internet would withstand centralization. Some gravitated toward factors like switching costs, which early on appeared to outweigh evidence that any firm had durable market power.[19] For example, in 2012 Robert Bork notably argued the proposition that "Google is the 'gateway' to the Internet . . . contradicts real world experiences [because] [c]onsumers can switch to other search engines at zero cost."[20] Those who see

14. Marin Armstrong, *How Many Websites Are There?*, STATISTA (Oct. 28, 2019), https://www.statista.com/chart/19058/how-many-websites-are-there/ [https://perma.cc/2SZ3-LEN2].

15. Robert B. Reich, Opinion, *Big Tech Has Become Way Too Powerful*, N.Y. TIMES (Sep. 18, 2015), https://www.nytimes.com/2015/09/20/opinion/is-big-tech-too-powerful-ask-google.html [https://perma.cc/9YPK-X9CX].

16. *See, e.g.*, David G. Post, *Governing Cyberspace*, 3 WAYNE L. REV. 155, 167 (1996) (describing the decentralized network of the Internet as allowing a "law of the Internet" to emerge "not from the decision of some higher authority, but as the aggregate of choices made by individual system operators about what rules to impose, and by individual users about which online communities to join."); John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND., (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/U5ZN-VM8K] (manifesto written in defiance of government regulation of the Internet, particularly the Telecommunications Act of 1996).

17. Nick Bilton, *One on One: Tim Wu, Author of 'The Master Switch'*, N.Y. TIMES: BITS (Nov. 4, 2010), https://bits.blogs.nytimes.com/2010/11/14/one-on-one-tim-wu-author-of-the-master-switch/ [https://perma.cc/BY8R-JPHR] (responding to interviewer in reference to the monopolies ABC, NBC, and AT&T).

18. *See* Katherine Griwert, *Google Dominates Search Engine Market*, BRAFTON (Apr. 8, 2010), https://www.brafton.com/news/google-dominates-search-engine-market-1260386 [https://perma.cc/W25A-L68T]; Erick Schonfeld, *U.S. Mobile Web Usage Grew 110 Percent Last Year*; *Apple Dominates, Android No. 2*, TECHCRUNCH (Jan. 5, 2010), https://techcrunch.com/2010/01/05/quantcast-mobile-web-apple-android/ [https://perma.cc/Q4RP-JBEC].

19. *See* Erick Schonfeld, *How Durable Are Information Monopolies on the Internet?*, TECHCRUNCH (Nov. 14, 2010), https://techcrunch.com/2010/11/13/information-monopolies-internet/ [https://perma.cc/67FB-8EZ8]. Switching costs in this context refer to the ease with which users can move from one website to the next.

20. Robert H. Bork & J. Gregory Sidak, *What Does the Chicago School Teach About Internet Search and the Antitrust Treatment of Google?*, 8 J. COMP. L. & ECON. 663, 667 (2012).

switching costs as enabling Big Tech's market power, rather than undermining it, have since criticized Bork's remarks.[21]

Today, many believe the Internet is concentrated because Big Tech consists of digital platforms,[22] while others argue that technology sectors, including the Internet, are too dynamic to remain beholden to monopoly power for too long.[23] The former opinion challenges the long-standing theory of "creative destruction," which characterizes industrial change as "incessantly revolutioniz[ing] the economic structure *from within*, incessantly destroying the old one, incessantly creating a new one."[24] Neither position has been definitively refuted and ultimately leave questions about competition in the digital marketplace unresolved.

As the digital world has shifted "from the wide-open web to semi-closed platforms," researchers and scholars have set out to understand the structural models that facilitated the move and enabled certain firms to capture market power and preserve it over time.[25] The following sections (II.B and II.C) provide an overview of the structural characteristics of digital platforms and how those characteristics enhance the market power of Big Tech.

B. The Characteristics of Big Tech

Big Tech companies are distinguished from other Internet-based companies because they are digital platforms. A digital platform is a two-sided market in which an intermediary (the platform) enables two interested

21. *See, e.g.*, Maurice Stucke, *Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data*, HARV. BUS. REV. (Mar. 27, 2018), https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data [https://perma.cc/8Y2Q-GZPX].

22. *See, e.g.*, COMMITTEE FOR THE STUDY OF DIGITAL PLATFORMS MARKET STRUCTURE AND ANTITRUST SUBCOMMITTEE, GEORGE J. STIGLER CENTER FOR THE STUDY OF THE ECONOMY AND THE STATE, REPORT 7–8 (July 1, 2019) https://www.judiciary.senate.gov/imo/media/doc/market-structure-report%20-15-may-2019.pdf [https://perma.cc/S366-F5ZJ] [hereinafter Stigler Report].

23. *See, e.g.*, David S. Evans & Richard Schmalensee, *Debunking the Network Effects Bogeyman*, 40 REGUL. 36 (2017).

24. JOSEPH SCHUMPETER, CAPITALISM, SOCIALISM AND DEMOCRACY 83 (1976). By comparison, while breakthroughs in technology that make farming more efficient can affect agriculture, the basis of it does not change; it will always be a matter of extracting matter from the earth.

25. Chris Anderson & Michael Wolff, *The Web Is Dead. Long Live the Internet*, WIRED (Aug. 17, 2010), https://www.wired.com/2010/08/ff-webrip/ [https://perma.cc/GJ4B-PWXF] (offering opposing views as to why the internet has shifted from a decentralized "wide-open web" to a network of more centralized "semi-closed" platforms).

parties, usually buyers and sellers, to interact.[26] Two-sided markets existed before the digital age,[27] but digital platforms are singled out for their strong network effects, economies of scale, and use of data.[28] Digital platforms are generally prone to tipping. Tipping means that once a firm gains enough users in a given market, it establishes itself as a powerful incumbent—one that is difficult to displace.[29] The popularity of digital platforms can be attributed to these characteristics which enable greater connectivity within Internet ecosystem.

1. Network Effects

Network effects occur when the value of a product is dependent upon the number of its users.[30] This occurrence is especially important for digital platforms because success hinges on the platform's ability to incentivize parties on either side (usually buyers and sellers) of the platform to interact. Once the number of users reaches a certain threshold, network effects take over and the service increases in value as more users join.[31] This phenomenon captures the trajectory of Facebook's growth: individuals' desire to be on the platform increases as more people they know join the network, linking the value of the social network to its size.

2. Economies of Scale

Economies of scale occur in industries when efficiencies in production reach a point at which production costs decrease with every added customer.[32] For example, when a manufacturer creates an assembly line that maximizes

---

26. *See* JEAN TIROLE, ECONOMICS FOR THE COMMON GOOD 379 (2017). Others define digital platforms as services that are "accessed via the internet [and operate as] two-sided or multi-sided platform[s], at least one side of which is open to the public and allows members of the public to produce content, buy and sell goods or services, or otherwise interact in ways that enable them to be more than simply passive consumers of goods and services." Harold Feld, *The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms*, ROOSEVELT INST. 30 (May 2019), https://rooseveltinstitute.org/wp-content/uploads/2020/07/RI-Case-for-the-Digital-Platform-Act-201905.pdf [https://perma.cc/6B9B-PZGM].

27. For example, credit cards are a two-sided market that allow consumers and merchants to transact such that merchants get instant payment while consumers get to defer payment to a later time. *See e.g.*, Ohio v. Am. Express Co., 138 S. Ct. 2274, 2277–78 (2017) (requiring consideration of cardholders and merchants in defining the relevant market of the two-sided credit-card market).

28. *See* Feld, *supra* note 26, at 31 (distinguishing Netflix from YouTube, both of which are two-sided platforms, because Netflix is simply "creating or licensing content and then making it available to consumers," whereas YouTube allows users to participate in content creation); Stigler Report, *supra* note 22, at 11–12.

29. Stigler Report, *supra* note 22, at 11–12.

30. *See* United States v. Microsoft, 253 F.3d 34, 49 (D.C. Cir. 2001) ("In markets characterized by network effects, one product or standard tends towards dominance, because 'the utility that a user derives from consumption of the good increases with the number of other agents consuming the good.'").

31. *See id.*

32. Stigler Report, *supra* note 22, at 36.

labor and materials efficiently and thus minimizes the cost of each product unit, the manufacturer reaches "scale." However, in typical markets, efficiencies have a ceiling that, once reached, will result in increased costs for every additional unit of production.[33] In digital markets, products and services are delivered as digital information and can be replicated at little to no cost.[34] An example of this is the digital distribution of music. Platforms like Spotify and Apple Music distribute millions of music albums with virtually zero increased cost to production because the music has no physical form—the costs do not increase in proportion to usership. "The same holds for information services that are subject to fixed design and development costs and fixed maintenance and updating costs."[35] For example, every time Facebook updates its services, it does so for all of its users in a jurisdiction, but the cost only incurs once.

Generally speaking, digital platforms enjoy "[i]ncreasing returns to scale."[36] After initial investment in fixed costs to create a service, a digital platform can generate profit as customers join the platform.[37] Once the platform has a large enough customer base, it enjoys lower average costs per customer, giving it a significant advantage over competitors that have not yet invested in the development of a new platform.[38] Network effects compound this occurrence because once a platform gains a significant number of users, those users are less likely to switch to another platform that has a smaller network of participants.[39] With platforms like Facebook and Google, which have strong network effects and economies of scale, competitors have less incentive to enter the market because the obstacles to reach a comparable size and profitability are difficult.[40]

3. The Role of Data

Data is an extremely valuable asset within the Internet ecosystem.[41] The analysis of data through machine learning and artificial intelligence creates value for companies "as it can guide the development of new products and services, predict the preferences of individuals, help tailor services and opportunities, and guide individualized marketing."[42] At the same time, advocates, academics, and others have raised concerns over how digital

33. *Id.*
34. *Id.*
35. *Id.*
36. *Id.*
37. *See id.*
38. Stigler Report, *supra* note 22, at 36.
39. *See id.*
40. *Id.*
41. Joris Toonders, *Data is the New Oil of the Digital Economy*, WIRED, https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ [https://perma.cc/X7LG-8NRL] (referring to data as "the new oil").
42. FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION i (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/EQ2D-AXPH].

platforms' control over user data may further cement market power.[43] Some summarize this phenomenon as a "virtuous loop":

> As a platform expands and diversifies, it obtains greater ability to compile different types of data from an increasing number of users. The benefits of these additional data will provide the platform with the opportunity to develop even more services and make enhancements to existing ones. Efficiency improvements further grow the user base and extent of collectible data. In this way, the platform may very well find itself in a sustained virtuous loop where success in one type of service leads to large scale data collection, which leads to more positive enhancements in services, then to further expansion and so-on.[44]

The role of data in the Internet ecosystem further complicates the dominance of digital platforms by amplifying the impact of network effects and scale. The mix of large data sets and the advantages of scale enable large firms to reap the benefits of artificial intelligence and machine learning at a faster and more dynamic rate than smaller companies.[45]

C. Concentration

The characteristics described above can create difficult conditions for competition, especially once a dominant firm establishes itself in a market.[46] When competitive markets function properly, "new enterprises [are] able to enter the market if they are more efficient or more innovative than the established monopoly," but in digital markets, research suggests that entrants cannot do so because the combination of qualities creates durable market power.[47] Once entry barriers exist, they can be difficult to overcome, and when such conditions exist for an extended period, there is potential that they will lead to poorer quality products and services and less innovation.[48]

Not only do the characteristics of Big Tech stifle competition, but many commentators, including the New Brandeisians, attribute consumer

---

43. *See* Eliana Garces & Daniel Fanaras, *Antitrust, Privacy, and Digital Platforms' Use of Big Data: A Brief Overview*, 28 J. OF THE ANTITRUST, UNFAIR COMPETITION, AND PRIV. L. SEC. OF THE CAL. LAW'S ASS'N, 23, 23 (2018).

44. *Id.* at 24–25 (noting that some literature assimilates the "virtuous loop" to network effects, but the phenomenon this literature refers to is the result of increasing returns to scale and scope in data, making the loop operative "for as long as additional data serves to make a service more efficient to every user.").

45. *See* Stigler Report, *supra* note 22, at 37.

46. *See id.* at 57 (explaining that absent entry barriers, "the tremendous amount of profit available . . . would stimulate entry").

47. *See* TIROLE, *supra* note 26, at 398.

48. Stigler Report, *supra* note 22, at 57.

exploitation, manipulation, and privacy violations to Big Tech's power.[49] However, the following section shows this is hardly the case.

D. Is Big Bad or Is Bad Bad?

Most of the Internet's magic happens behind the shroud of Big Tech. Seamless surfing between webpages that offer tailor-made recommendations are conveniences powered by what some refer to as the one-way mirror of corporate surveillance.[50] Big Tech has been accused of having a stranglehold on data, but it is not the only group collecting it. From shopping centers to concert venues and car dealerships, many unsuspecting industries participate in corporate surveillance.[51] However, most data tracking goes undetected by consumers and many of the companies involved do not interact directly with them.[52]

1. Data Collection Practices Across the Internet and Beyond

There are two categories of information that travel over the Internet. "First-party data" is information collected by companies when people interact directly with their services.[53] "Third-party data" is information collected by a company from any place other than through direct interactions with users.[54] A good illustration of this is Facebook, which learns about users through first-party data because of what they like, click on, and post on its platform. But Facebook also collects third-party data about people across the Internet using Facebook Pixel, which is a tracking device installed on thousands of different websites that allows Facebook to collect data about individuals' activities online.[55] Like Facebook Pixel, third-party data is collected all the time and in every corner of the Internet.[56] The more time people spend online, the more valuable data becomes. But Big Tech firms are not the only ones cashing in.[57]

Data brokers are "companies whose primary business is collecting personal information about consumers from a variety of sources and

---

49. *See id.* ("when platforms do not face competition, they will be able to reduce quality, for example, by decreasing privacy protections, without losing customers or revenue.").

50. BENNET CYPHERS & GENNIE GEBHART, ELECTRONIC FRONTIER FOUNDATION, BEHIND THE ONE-WAY MIRROR: A DEEP DIVE INTO THE TECHNOLOGY OF CORPORATE SURVEILLANCE (Dec. 2, 2019), https://www.eff.org/document/behind-one-way-mirror-deep-dive-technology-corporate-surveillance [https://perma.cc/Z6XR-BVYF]; *see also* Shoshana Zuboff, *Big Brother: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75 (2015).

51. *See* CYPHERS, *supra* note 50, at 4.

52. *See id.*

53. *Id.* at 4–5.

54. *Id.*

55. *See* Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook*, CONSUMER REPS., (Apr. 11, 2018), https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook/ [https://perma.cc/8U6K-NR2P].

56. *See Id.*

57. *See id.*

aggregating, analyzing, and sharing that information, or information derived from it" for a wide range of purposes including, but not limited to, "marketing products, verifying an individual's identity, or detecting fraud."[58] Some laws regulate data broker activity in specific industries. For example, the Fair Credit Reporting Act ("FCRA") governs companies providing consumer data to credit reporting agencies or for credit related purposes like employment, insurance, and housing.[59] However, there is no federal law covering the use of consumer data for marketing purposes, which includes e-commerce and any online ad-supported goods and services, which comprise the majority of the Internet ecosystem.

Data brokering is believed to be a $200 billion industry,[60] and even firms like Facebook and Google are customers "because of the wealth and granularity of offline and cross-device data [brokers] have accumulate[d]."[61] One company, PeekYou, uses technology to analyze content from different social sites, news sources, homepages, and blog platforms to build profiles of the individuals it identifies.[62] Acxiom, another data broker, collects data from over 60 countries, and has 2.5 billion addressable consumers with over 10,000 attributes compiled for those consumers.[63]

The main difference between data brokers and Big Tech is that many brokers do not collect data directly from consumers. Instead, data brokers collect data from public government sources, other publicly available sources, and commercial sources online and offline.[64] This allows them to build a "detailed composite of a consumer's life" from seemingly disparate data points gathered from a wide range of a consumer's online and offline activities.[65] Many people are likely unaware that this practice is legal, however in 2019, the U.S. Court of Appeals for the Ninth Circuit held that hiQ, a data analytics company, could scrape publicly available data from LinkedIn without reprisal.[66]

58. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i, 3 (May 2014) [hereinafter FTC Data Broker Report].

59. *Id.* at i.

60. David Lazarus, *Column: Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, L.A. TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers [https://perma.cc/57BY-RPF8].

61. Aliya Ram & Madhumita Murgia, *Data Brokers: Regulators Try to Reign in the 'Privacy Deathstars'*, FIN. TIMES (Jan. 7, 2019), https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521 [https://perma.cc/9D3A-Q3SD].

62. *About Us*, PEEKYOU, https://www.peekyou.com/about/ (last visited Apr. 4, 2020) [https://perma.cc/6PGE-DBHG].

63. *What We Do*, AXCIOM, https://www.acxiom.com/what-we-do/data/ (last visited Apr. 4, 2020) [https://perma.cc/A8B9-NM8L].

64. FTC Data Broker Report, *supra* note 58, at 11.

65. *Id.*

66. hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019).

2. Commercial Data Collection Leaves Consumers Exposed

Data is fundamental to the basic functions of the Internet.[67] It allows companies to provide Internet services for free and plays an important role in the advancement of existing technology infrastructures.

There is also the potential for data to be used for nefarious purposes. There are many allegations that digital platforms employ data collected in the commercial context in a "deeply intentional and highly consequential" regime aimed "to predict and modify human behavior as a means to produce revenue and market control."[68]

Up until now, the business of collecting consumer data has operated under a shroud of secrecy. Big Tech has been a target for blame for because it is big and has considerable influence over much of the Internet. But a policy agenda focused on market share and power risks making size the disease such that it becomes the proxy for consumer harm online.

The New Brandeis School and others calling for antitrust intervention mistakenly focus on the structure of Big Tech as the means to cure the harms associated with it. However, the issue is behavioral, not structural, and as shown above, the behavior is common throughout the Internet ecosystem.

The historical perspective provided in the next section shows that focusing antitrust doctrine on the structure of markets rather than welfare outcomes,[69] as is its traditional function, will fail to address consumer exploitation, manipulation, and privacy violations online.

III. THE MOVEMENT TO TAKE DOWN BIG TECH

In the last year, criticism that Big Tech is too big and too powerful has intensified[70] with calls to action gaining bipartisan support.[71] Perhaps the most progressive advocates are the antitrust experts and scholars organized under the New Brandeis School. While opinions differ on what to do about Big Tech, the consensus is *something* should be done. Among the most radical and often quoted solution is "break them up." Some advocate for the traditional approach: a structural splitting of these firms into their component businesses, such as, for example, breaking up Amazon into Amazon

67. *See* Zachary Karabell, *Don't Break Up Big Tech*, WIRED (Jan. 23, 2020), https://www.wired.com/story/dont-break-up-big-tech/ [https://perma.cc/45M6-2UHA] (suggesting that in order for businesses to thrive under a different model, they would have to charge customers more for services than customers have so far been willing to pay).

68. Zuboff, *supra* note 50, at 75.

69. *See infra* III.B.

70. *See, e.g.*, STAFF OF H. SUBCOMM. ON ANTITRUST, COMMERCIAL AND ADMIN. LAW OF THE COMM. ON THE JUDICIARY, INVESTIGATION OF COMPETITION IN DIG. MKTS., 116th Cong. (2020).

71. *See* Christopher Mims, *Republicans and Democrats Find a Point of Agreement: Big Tech Is Too Powerful*, WALL ST. J. (July 30, 2020), https://www.wsj.com/articles/republicans-and-democrats-find-a-point-of-agreement-big-tech-is-too-powerful-11596118625 [https://perma.cc/64E5-5X3U].

Marketplace, Amazon Web Services, and AmazonBasics.[72] Others have argued that Big Tech's vertically integrated parts should be unbound so none of the firms can own a platform that allows merchants and consumers to buy and sell while also selling its own products on the platform.[73] Others want to see enforcement officials unwind mergers viewed as anticompetitive.[74]

A. Shifts within Congress and Federal Agencies

Frustrations about the power of Big Tech have been percolating for years among policy groups, academic scholars, and antitrust experts, finally boiling over in 2019. Senator Elizabeth Warren (D-MA), was one of the first in Congress to formulate a plan to take on Big Tech. Her two-part proposal creates "Platform Utilities" of firms with over $25 billion (capturing all of Big Tech) in global revenue and prohibits those firms from operating and participating on the same platform.[75] Her plan also designates regulators to reverse anticompetitive mergers.[76]

The intrigue of antitrust action is the blunt force of the Sherman Act, which is one of the government's main tools capable of stopping corporations from amassing too much power. However, monopolization cases are complex, require considerable resources, and could take years to conclude. However, Senator Warren's allegations that Big Tech has "bulldozed competition, used our private information for profit, and tilted the playing field against everyone else,"[77] and Republican Senator Josh Hawley's (R-MO) remarks that "they've given us some of the worst of America,"[78] display considerable motivation from lawmakers to crack down on Big Tech.

A similar consensus was on display at a 2020 congressional hearing by the House of Representative's Subcommittee on Antitrust, Commercial, and Administrative Law, where top executives from smaller technology companies testified about the different tactics tech giants—particularly Google, Apple, and Amazon—employ to crush their competitors.[79] Led by

---

72. *See* Steve Lohr, *How Should Big Tech Be Reined In? Here Are 4 Prominent Ideas*, N.Y. TIMES (Aug. 20, 2019), https://www.nytimes.com/2019/08/20/technology/big-tech-reined-in.html [https://perma.cc/XU76-6JTP].

73. *Id.*

74. *Id.*

75. *See* Elizabeth Warren, *Here's How We Can Break Up Big Tech*, MEDIUM (Mar. 8, 2019), https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c [https://perma.cc/4EF4-E3AH].

76. *See id.*

77. *Id.*

78. Matt Laslo, *Josh Hawley Says Tech Enables 'Some of the Worst of America'*, WIRED (Aug. 16, 2019), https://www.wired.com/story/josh-hawley-tech-enables-worst-of-america/ [https://perma.cc/8AAT-4KP2].

79. One example of bullying tactics came from testimony by Tile, Inc. representatives, who testified about Tile's experience with Apple's anti-competitive practices. According to Tile, Apple abruptly informed Tile that Apple would no longer carry Tile products in its stores because it created its own Tile-like products. *See Online Market Platforms and Market Power, Part 5: Competitors in the Digital Economy, Hearing Before Subcomm. on Antitrust, Com. and Admin. L. of the H. Comm. on the Judiciary*, 116th Cong. (2020) (testimony of Kirsten Daru, Chief Privacy Officer and General Counsel, Tile Inc.).

Chairman David Cicilline (D-RI), the subcommittee began investigating Big Tech in 2019, looking for answers to how these companies amassed so much wealth and whether it accumulated through anticompetitive or illegal means. The Subcommittee released its report in October 2020 with recommendations on how to correct digital platform market dominance including antitrust reform, structural separation of dominant firms, and the implementation of rules to prevent firms from discriminating and self-preferencing.[80]

In response to pressure from Congress and the public, the FTC and DOJ opened probes into Big Tech and have since brought suit against Facebook and Google respectively.[81] The FTC also issued a broad Section 6(b) order to social media and video streaming platforms in December 2020 that could serve as the basis for future lawsuits.[82] Both agencies have recently been scrutinized for having lax enforcement agendas over the last two decades,[83] although it appears the tides are changing given the recent lawsuits. Still, the dissatisfaction with these institutions is deeper than simply years of bad leadership and management. Couched within the debate on what to do about Big Tech is a meta-debate over whether the doctrine to take down monopolies is itself up to the job.

B. The Evolution of Antitrust and the Rise of the New Brandeis School

Within the debate on what to do about Big Tech is a deeper divide over antitrust doctrine. On the one side is the Chicago School, which has dominated antitrust jurisprudence in the courts and agencies since the 1970s, and on the other is the New Brandeis School—a populist movement that looks to replace the Chicago School's consumer welfare standard with a broader set

---

80. *See* STAFF OF SUBCOMM. ON ANTITRUST, COM. AND ADMIN. L. OF THE COMM. ON THE JUDICIARY, INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 375–402 (2020). Congressman Ken Buck (R-CO) released a report in response to the majority staff's report that details alternative solutions to Big Tech dominance. *See* STAFF OF SUBCOMM. ON ANTITRUST, COM. AND ADMIN. L. OF THE COMM. ON THE JUDICIARY, THE THIRD WAY: ANTITRUST ENFORCEMENT IN BIG TECH (2020).

81. *See* FTC v. Facebook, Inc. (D.D.C filed Dec. 9, 2020); United States v. Google LLC, No. 1:20-cv-3010, 3 (D.D.C. filed Oct. 20, 2020). The FTC is still working on an antitrust probe into Amazon and the DOJ is still working on a probe into Apple. *See* Laslo, *supra* note 78.

82. *FTC Issues 6(b) Orders to Social Media and Video Streaming Services*, FTC, https://www.ftc.gov/news-events/blogs/business-blog/2020/12/ftc-issues-6b-orders-social-media-video-streaming-services (last visited 1/1/2021) [https://perma.cc/WP4E-DBMQ] (the order covers social media and video streaming services by Amazon, Discord, Facebook, Reddit, Snapchat, TikTok, Twitter, WhatsApp, and YouTube).

83. *See* Kadhim Shubber, *U.S. Antitrust Enforcement Falls to Slowest Rate Since 1970s*, FIN. TIMES (Nov. 28, 2018), https://www.ft.com/content/27a0a34e-f2a0-11e8-9623-d7f9881e729f []; Jason Del Rey, *Why Congress's Antitrust Investigation Should Make Big Tech Nervous*, VOX (Feb. 6, 2020), https://www.vox.com/recode/2020/2/6/21125026/big-tech-congress-antitrust-investigation-amazon-apple-google-facebook [https://perma.cc/24VU-MQ3S]. ("The last major antitrust battle between the US government and a tech giant ended in 2013 when the FTC cleared Google of violating antitrust law in relation to how it ranks and displays search results from competing websites like Yelp and TripAdvisor.")

of measures to fight against what Supreme Court Justice Louis Brandeis coined "the curse of bigness."[84]

"There [is] a long tradition of fear of monopoly in the United States."[85] Between 1850 and 1900, the U.S. saw the climax of laissez-faire policy.[86] It was a period of tremendous social and economic upheaval—improvements in transportation and communications revolutionized the economy and society—and business growth outpaced the development of the law.[87] The notorious trusts formed in the wake of the development, harnessing economic power to dominate industries and politics.[88] People turned against monopolies because they led to higher prices, suppression of wages, decreased innovation, and less productivity.[89]

The Progressive Era (1880-1920) arose in reaction to the rise of monopoly power.[90] Legal thinkers at the time began to question the philosophy of laissez-faire,[91] pointing out that although industrialization showed promise as an economic model, "[the] premise that unregulated self-interest would yield optimal economic development had never been proven," and in certain industries, such as the railroads, "laissez-faire seemed not to work."[92] Combined with renewed concerns for public welfare and social reform, the Progressive Era ushered in ideas about wealth and corporate power that American society still grapples with today, and are center stage in the Big Tech debate.

Progressive economists at the turn of the 20th century were greatly concerned with unequal distributions of wealth.[93] "The major legal innovations arising from that period—antitrust, corporate governance, and public utility—were . . . parallel strategies for addressing different forms of private power . . . [and] share[d] a common moral purpose: not just to facilitate market mechanisms or promote efficiency, but to ensure the accountability of private power and to promote public values such as access, equity, and innovation."[94] The Supreme Court has noted:

---

84. *See* Lina Khan, Editorial, *The New Brandeis Movement: America's Antimonopoly Debate*, 9 J. OF EUR. COMPETITION L. & PRAC. 131, 131–32 (2018).

85. LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 463 (2d. ed., 1985).

86. *Id.* at 440.

87. *See id.*

88. *See id.* at 463–64.

89. *See generally id.*

90. *See* Jean-Paul Simon, *The Origins of US Public Utilities Regulation: Elements for a Social History of Networks*, 1993 FLUX 33.

91. *See* Herbert Hovenkamp, *The First Great Law and Economics Movement*, 42 STAN. L. REV. 993, 998 (1990).

92. *Id.*

93. *See* K. Sabeel Rahmen, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621, 1621 (2018).

94. *Id.* at 1634.

> The Sherman Act was designed to be a comprehensive charter of economic liberty. . . . It rests on the premise that the unrestrained interaction of competitive forces will yield the best allocation of our economic resources, the lowest prices, the highest quality and the greatest material progress, while at the same time providing an environment conducive to the preservation of our democratic political and social institutions.[95]

The Sherman Act of 1890 is notoriously vague. Section 2 states in part: "Every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize . . . shall be deemed guilty of a felony. . . ."[96] Due to its open-endedness, antitrust jurisprudence has vacillated throughout its 130 years of development while at the same time maintaining the principle that the statutes themselves are a charter of economic liberty.[97]

Modern Section 2 jurisprudence is nearly synonymous with the Chicago School's consumer welfare standard. The Chicago school of thought gained popularity in the 1970s for its streamlined economic approach to the application of antitrust law at a time when critics questioned the government's interventionist policies.[98] Robert Bork, the Chicago School pioneer who originated the consumer welfare standard, was at the forefront of the effort to expose the failures he and others[99] observed in the judicial process—namely the inconsistent and confusing precedent set by the Court's embrace of broad and diverging social, political, and ethical values.[100] He argued that "antitrust was unworkable" when it was used to promote a diverse set of goals, which

---

95. N. Pac. Ry. Co. v. United States, 356 U.S. 1, 4 (1958).

96. 15 U.S.C. § 2.

97. *See generally* William E. Kovacic, *Failed Expectations: The Troubled Past and Uncertain Future of the Sherman Act as a Tool for Deconcentration*, 74, IOWA L. REV. 1105 (1989) (identifying over time a cyclical pattern in policy agendas that mark the periods of American government efforts to use the Sherman Act to deconcentrate markets).

98. William F. Adkinson, Jr. et al, FED. TRADE COMM'N, ENFORCEMENT OF SECTION 2 OF THE SHERMAN ACT: THEORY AND PRACTICE, WORKING PAPER 10 (Nov. 3, 2008) (enforcement agencies acted aggressively during the 1960s and 70s but lost many cases, which raised doubts about the economic theories underlying those cases); *see also,* Richard A. Posner, *The Chicago School of Antitrust Analysis*, 127 UNIV. PA L. REV. 925, 928–29 (1979) ("in the 1950's and early 1960's . . . [c]asual observation of business behavior, colorful characterizations (such as the term 'barrier to entry'), eclectic forays into sociology and psychology, descriptive statistics, and verification by plausibility took the place of careful definitions and parsimonious logical structure of economic theory.").

99. *See, e.g.*, Richard A. Posner, *The Chicago School of Antitrust Analysis*, 127 U. PA. L. REV. 925, 926 (1979) (arguing that the Chicago and Harvard schools of thought did not "emerge from a full-blown philosophy of antitrust. Rather, they were the product of pondering specific questions raised by antitrust cases, and only in retrospect did it become clear that they constituted the basis of a general theory of the proper scope of antitrust policy."). Posner agreed with the Chicago School posture.

100. *See* Robert H. Bork, *Legislative Intent and the Policy of the Sherman Act*, 9 J.L. & ECON. 7, 8 (1966) (referring to a Second Circuit opinion that held a company violated Section 2 of the Sherman Act on the basis of "belief that great industrial consolidations are inherently undesirable, regardless of their economic results." Bork noted the opinion failed "to explain what the noneconomic helplessness of the individual might consist of, what category of individuals was involved, or how the concept applied to the facts of the case. . . .").

was why he promoted a single-minded focus on consumer welfare.[101] The theoretical premise is that "a practice restrains trade, monopolizes, is unfair, or tends to lessen competition if it harms consumers by reducing the value or welfare they would have obtained from the marketplace absent the practice."[102]

Robert Bork and his contemporaries shifted antitrust doctrine towards policies that embrace vertical integration[103] and business expansion across markets[104] because they serve economic efficiencies and development that ultimately benefit consumers.[105] Today, when courts analyze challenged conduct, they tend to focus on whether the behavior affects economic efficiencies and will resist a ruling that may discourage dominant firms from advancing business strategies that improve consumer welfare at the expense of competitors.[106] As noted by the Supreme Court, "the antitrust laws . . . were enacted for 'the protection of competition, not competitors."[107]

Practically speaking, maintaining the "competitive process" is an abstraction. It is attractive in theory but less so as a real-world application because it results in winners and losers, where the losers' livelihoods suffer. With this in mind, the question becomes what is the most important group to protect in carrying out this end? "If antitrust law is required to maximize

---

101. *See* Gregory J. Werden, *Back to School: What the Chicago School and New Brandeis School Get Right*, SYMP.ON RE-ASSESSING THE CHI. SCH. OF ANTITRUST L. 5 (2018). Bork argued that "[n]ot only was consumer welfare the predominant goal expressed in Congress, but the evidence strongly indicates that, in case of conflict, other values give way before it. This means that such other values are superfluous to the decision of cases since none of them would in any way alter the result that would be reached by considering consumer welfare alone." Bork, *supra* note 100, at 10–11.

102. Thomas G. Krattenmaker et al, *Monopoly Power and Market Power in Antitrust Law*, 76 GEO L.J. 241, 244 (1987).

103. Vertical integration refers to the combination of a firm's assets along a single supply chain. It may lead to anticompetitive conduct in certain contexts where it enables a dominant firm to foreclose a rival's access to parts of the supply chain or raise a rival's costs by increasing the price of a certain product. *See* U.S DEP'T OF JUSTICE & FED. TRADE COMM., VERTICAL MERGER GUIDELINES 1, 4 (June 30, 2020), https://www.ftc.gov/system/files/documents/reports/us-department-justice-federal-trade-commission-vertical-merger-guidelines/vertical_merger_guidelines_6-30-20.pdf [https://perma.cc/DR2J-5DXD].

104. Examples of this are tie-ins, which is when a company offers products together as part of a package. This "can benefit consumers who like the convenience of buying several items at the same time . . . [it] can also reduce manufacturer's costs for packaging, shipping, and promoting the products" among other efficiencies. *See Tying the Sale of Two Products*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/single-firm-conduct/tying-sale-two-products (last visited, Apr. 10, 2020) [https://perma.cc/4WHX-CYAG]. Tie-ins can also be used anticompetitively. For example, "a monopolist may use forced buying, or 'tie-in' sales, to gain sales in other markets where it is not dominant and to make it more difficult for rivals in those markets to obtain sales." *Id.*

105. *See* Donald F. Turner, *The Durability, Relevance, and Future of American Antitrust Policy*, 75 CAL. L. REV. 797, 809 (1987).

106. William E. Kovacic, *The Intellectual DNA of Modern U.S. Competition Law for Dominant Firm Conduct: The Chicago/Harvard Double Helix*, 2007 COL. BUS. L. REV. 2, 19–20 (2007).

107. Brunswick Corp. v. Pueblo-Bowl-O-Mat*,* 429 U.S. 477, 488 (1977) (quoting Brown Shoe Co. v. United States, 370 U.S. 294, 320 (1962)); *see also S*pectrum Sports v. McQuillan, 506 U.S. 447, 458 (1993).

simultaneously the welfare of small communities, the number of Mom-and-Pop stores, the absolute freedom of entry . . . workers' leisure time, and the ability of firms to avoid competing with each other, then antitrust law is paralyzed."[108] Therefore, the Chicago School places the consumer at the center of antitrust analysis. Over the years, the courts and enforcement agencies have, for the most part, faithfully adhered to the consumer welfare standard. Today, the debate about its viability in addressing concentration in the digital marketplace is enmeshed in the debate about the power of Big Tech.

New Brandeisians reject the consumer welfare standard, which they believe has led antitrust jurisprudence astray and resulted in damage to the American economy.[109] Lina Khan, a prominent New Brandeisian, argues that the Chicago School's consumer welfare theory is "antithetical to the goal of competition" because its focus on efficiency emphasizes economic outcomes rather than maintenance of the competitive process.[110] Using the philosophical and social foundations of Progressive Era ideals, New Brandeisians argue for a new (or rather old, depending on the scholarship) framework for antitrust doctrine[111]—one recognizing "that concentrated private power [is] a menace, a barrier to widespread prosperity, and an indefensible division of the spoils of progress and economic security that yields human flourishing."[112] The New Brandeis School, like Brandeis, believes "that the *structure* of our markets and of our economy can determine how much real liberty individuals experience in their daily lives."[113]

Some critics push back on the notion that antitrust doctrine is inadequate to handle Big Tech's anticompetitive conduct.[114] At a conference in June 2019, Assistant Attorney General of the DOJ Antitrust Division, Makan Delrahim, reviewed the many successful antitrust cases against

---

108. Krattenmaker, *supra* note 102, at 244.

109. *See, e.g.*, Lina Khan, *Ideological Roots of America's Market Power Problem*, 127 YALE L.J. 960, 964 (2018) ("The sweeping market power problem we confront today is a result of the current antitrust framework. The enfeebled state of antitrust enforcement traces directly to an intellectual movement that fundamentally rewrote antitrust law—redefining its purpose, its orientation, and the values that underlie it.").

110. *Id.* at 968.

111. One of the movement's leading thinkers, Tim Wu, has advocated extensively for reviving the anti-monopoly tradition in the U.S. which he believes has been obliterated by the economic policies of the last 40 years. *See* Tim Wu, *The Utah Statement: Reviving Antimonopoly Traditions for the Era of Big Tech*, MEDIUM ONEZERO (Nov. 18, 2019), https://onezero.medium.com/the-utah-statement-reviving-antimonopoly-traditions-for-the-era-of-big-tech-e6be198012d7. [https://perma.cc/C67H-NR6N].

112. *Id.*; *but see* Joshua D. Wright et al., *Requiem for a Paradox: The Dubious Rise and Inevitable Fall of Hipster Antitrust*, 51 ARIZ. ST. L.J. 293 (2019) (arguing that "[o]ver the last fifty years, antitrust has developed into a coherent, principled, and workable body of law that contributes positively not only to American competitiveness and societal well-being, but also helps to export the culture of market competition around the world.").

113. Khan, *supra* note 84, at 131 (arguing that the Chicago School's focus on consumer welfare has distorted the doctrine to prioritize outcomes—welfare of the consumer—instead of ensuring the market structure supports the competitive process) (emphasis added).

114. *See, e.g.*, Joe Kennedy, *Why the Consumer Welfare Standard Should Remain the Bedrock of Antitrust Policy*, INFO. TECH. & INNOVATION FOUND., http://www2.itif.org/2018-consumer-welfare-standard.pdf [https://perma.cc/G495-6D3V].

legitimate monopolization and warned against dispatching antitrust laws to address issues unrelated to competition.[115] His remarks highlight the struggle over defining the purpose and aim of antitrust. This dispute traces directly to the vague language of the Sherman Act. As explained above, the Act was passed with tremendous public support. Ultimately, it is a law shaped by public policy and will continue to be shaped by public policy.

IV. BREAKING UP BIG TECH WILL NOT CURE CONSUMER HARMS

The intellectual divide in antitrust policy breaks at the fine line that defines the difference between procompetitive and anticompetitive conduct.[116] The Sherman Act itself causes this issue in part because it does not define what it means "to monopolize" or "attempt to monopolize."[117] Legislative history[118] and the courts affirm that monopolies are not illegal per se.[119] Likewise, courts acknowledge that "monopoly may be obtained by superior skill and unmatched effort."[120] Herbert Hovenkamp, a notable antitrust scholar, helped elucidate the distinction between illegal and legal monopolization. He points out that "in most circumstances involving monopoly, the 'intent' to create a monopoly anticompetitively cannot be distinguished from the intent to do so competitively."[121] Here, he simply refers to how normal business conduct works in competitive markets; a firm "intends" to increase its profits which, if successful, invariably leads to excluding profits from other firms.[122] If the market is competitive, and many firms are vying for market share, it is harder to conclude that competitive conduct is intended to harm any particular rival.[123] In a concentrated market, this scenario looks different. When a dominant firm has few competitors and it "intends" to increase its profits, it likely does so with the awareness that its actions will harm rivals. However, this scenario does not necessarily lead to the conclusion of intentional harm either.[124] The goal of business is well

115. Makan Delrahim, U.S. Assistant Att'y Gen., Remarks at the Antitrust New Frontiers Conference (Jun. 11, 2019) (transcript available at https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-antitrust-new-frontiers [https://perma.cc/X7UG-L8W9]).

116. *See* Herbert Hovenkamp, *The Monopolization Offense*, 61 OHIO STATE L.J. 1035, 1036 (2000).

117. *Id.* at 1035 (adding that "the legislative history of the antitrust laws provides no enlightenment about what it means 'to monopolize' a part of commerce").

118. *Id.* at 1035–36 (At the time the statute passed, some "objected that the plain language of the statute would condemn one 'who happens by his skill and energy to command an innocent and legitimate monopoly of a business.'").

119. Adkinson, *supra* note 98, at 1.

120. *Id.* at 1. Conduct that can be characterized as a violation includes that which is done in order to acquire a monopoly position or maintain a monopoly position, and which exposes consumers to the harmful effects of monopoly, such as increased prices or decreased output.

121. Hovenkamp, *supra* note 116, at 1039.

122. *See id.*

123. *See id.*

124. *See id.* at 1039–40.

understood. Companies big and small are formed to make money. Therefore, in monopolization cases adjudicators are pressed to determine when a dominant firm's profit-seeking conduct and market share exceed the benefits associated with it.[125]

New Brandeisians claim that the competitive process is best protected by "structural conditions (competition) as a way of promoting a set of outcomes and principles" such as "preventing unfair wealth transfers from consumers, producers and workers to monopolistic firms; preserving open markets in order to ensure opportunity for entrepreneurs; and halting excessive concentrations of private power."[126] However, this structural framework ignores the fine line between procompetitive and anticompetitive acts and, under certain circumstances, could be employed to prevent behavior that enhances competition.

New Brandeisians not only overemphasize the role of structure in maintaining healthy and competitive markets, they also mistakenly entangle the goal of protecting the competitive process with remedying consumer exploitation, manipulation, and privacy violations associated with the concentration of Big Tech.[127]

Digital platforms have deep insight into their respective markets because they are uniquely positioned to gather data on both sides of the transactions they administer. More often than not, consumers are unaware how much of their online activity is being tracked and used to sell them products and services.[128] However, data is essential for operating in the Internet ecosystem today and it allows companies to offer a variety of high-quality services.[129]

Despite the importance of data to online business operations, some allege that Big Tech may use data to exploit consumers. Data mining, machine learning, and algorithmic pricing practices are claimed to disrupt the natural functioning of the market by inhibiting consumers from making informed purchasing decisions and allowing firms to unfairly maximize profit from each transaction.[130] The presumption is that the amount of data Big Tech controls, combined with its "ability to control the environment and the timing

125. *Id.* at 1040.

126. Khan, *supra* note 109, at 971–72, n.52.

127. Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and the Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 849, 889 (2014).

128. *Id.* at 849, 861–62, n.44.

129. *See generally* Christiane Lehrer et al., *How Big Data Analytics Enables Service Innovation: Materiality, Affordance, and the Individualization of Service*, 35 J. OF MGMT. INFO. SYS. 424 (2018).

130. *Id.* at 854, 859 (explaining that the technology employed does not allow for a "single equilibrium price" making it impossible for antitrust enforcers to determine how price discrimination is being deployed and whether it actually benefits consumer welfare).

of choices and offers," creates a system in which consumers are essentially powerless.[131]

In *Amazon's Antitrust Paradox*, Khan notes that Amazon's control over vast amounts of data "enables it both to extend its tug over customers through highly tailored personal shopping experiences, and, potentially, to institute forms of price discrimination,"[132] in which customers will see different prices for the same products based on information gathered about them.[133] Journalists note the confusion that arises when Amazon and other online services constantly shift prices day-to-day and sometimes even hour-to-hour.[134] Behavioral economists also raise issue with Big Tech's ability to exploit and manipulate inherent consumer biases.[135] Commentators note that the value Google delivers to users in the form of information is "delivered by [its] access to other people's labor and knowledge, most of which Google accesses for free itself."[136] When Google turns the information into behavioral profiles for advertisers, it has the potential to cause "the kind of predatory marketing we saw in the subprime housing bubble globally and in a range of other sectors" where "seedier companies . . . target the most naïve and vulnerable potential consumers and facilitate new forms of price discrimination."[137] Even with the potential for abuse, research shows that price discrimination is common in many markets and is actually an efficient practice that, in many instances, enhances market competition.[138]

---

131. *See* Stigler Report, *supra* note 23, at 59; *but see* Diane Coyle, *Practical Competition Policy Implications of Digital Platforms*, 82 ANTITRUST L.J. 835, 842 (2019) (recognizing the validity of concerns about how pricing algorithms work "given their black box character" but affirming that there is no evidence to conclude that price discrimination is currently causing harm to consumers).

132. Lina Kahn, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 788 (2017) ("Not only has Amazon inaugurated an entire generation into online shopping through its platform, but it has expanded into a suite of additional businesses and amassed significant droves of data on users . . . and control over data equip an incumbent platform to recoup losses in ways less obviously connected to the initial form of below-cost pricing."). Khan claims, "Amazon's conduct suggests predatory pricing and integration across related business lines are emerging as key paths to establishing dominance—aided by the control over data that dominant platforms enjoy." *Id.* at 789.

133. *See* ORGANISATION FOR ECON. CO-OPERATION AND DEVELOPMENT, DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS COMPETITION COMMITTEE, PERSONALIZED PRICING IN THE DIGITAL ERA—NOTE BY THE UNITED STATES 3 (Nov. 21, 2018), https://one.oecd.org/document/DAF/COMP/WD(2018)140/en/pdf [https://perma.cc/2LT9-2KNV] [hereinafter OECD Report].

134. *See* Jerry Useem, *How Online Shopping Makes Suckers of Us All*, THE ATL. (May 2017), https://www.theatlantic.com/magazine/archive/2017/05/how-online-shopping-makes-suckers-of-us-all/521448/ [https://perma.cc/9RLN-HFQF].

135. Stigler Report, *supra* note 22, at 58–60 (explaining that "[f]raming, nudges, and defaults can direct a consumer to the choice that is most profitable for the platform" which exemplifies their ability "to understand and manipulate individual preferences at a scale that goes far beyond what is possible in traditional markets").

136. Newman, *supra* note 127, at 857.

137. *Id.*

138. *See* OECD Report, *supra* note 133, at 2, (noting that "[i]n certain limited circumstances, price discrimination might feature as an aspect of an exclusionary strategy meant to enhance or protect market power. Intervention should be limited to preventing these exclusionary abuses.").

The dangers associated with these data collection practices are well documented. However, much of the analysis fails to make the case that consumer manipulation and exploitation are problems related to the *bigness* of Big Tech. As stated in Section II.D, the allegedly exploitative practices actually pervade the entire online ecosystem with companies of all sizes.

Those who view alleged exploitation as a distinctly Big Tech issue attempt to show that large-scale collection of data entrenches the strength of Big Tech, thereby effectuating harm. For example, Google products like Gmail, Google Search, YouTube, and even Google Chrome effectively gather data about individuals "across almost every imaginable space where users operate online" and "[g]iven how valuable such profiling is to advertisers, Google's entrenched knowledge of consumers' personal information makes it nearly impossible for any rival or potential rival to woo online advertisers away and creates an anticompetitive barrier to entry."[139] In this case, Google's dominance is elemental to the harm. However, the amount of data the company possesses is not the impetus of the abuse. It may be true that Google has an extensive control over consumer data that disrupts competition in the advertising market, but dismantling Google's conglomerate will not change the potential for consumer manipulation and exploitation online because the components of a hypothetically broken-up Google would still collect the same data on their own. The same is true for Amazon's business; whenever there exists a buyer-seller relationship online, asymmetries of information will exist, and depending on how often a consumer uses a particular online service, that company may have more or less potential to use the information it gathers to advantage itself in a transaction.

Privacy is another category of harm associated with Big Tech's dominance. Privacy, like quality, is recognized as a non-price dimension of competition, but measuring how prominently privacy factors into consumer decision-making is hard to calculate.[140] Privacy could be a factor to consider in a merger review or a monopolization case where a transaction or conduct "generate[s] market power [that] . . . may harm consumers when it results in diminished quality, selection, or service."[141] Privacy concerns were a focus in the FTC's review of Google's 2007 acquisition of the advertising technology firm DoubleClick.[142] Critics of the transaction raised questions about the boundaries of privacy and consumer expectations because the combination of

139. Nathan Newman, *Search, Antitrust, and the Economics of the Control of User Data*, 31 Y.J. REG. 401, 407 (2014).

140. Maurice Stucke & Allen P. Grunes, *No Mistake About It: The Important Role of Antitrust in the Era of Big Tech*, THE ANTITRUST SOURCE 4 (April 2015).

141. Fed. Trade Comm'n, File No. 071-0170, Statement of Federal Trade Comm'n Concerning Google/DoubleClick 1–2 (2007) [hereinafter FTC Statement on Google/DoubleClick].

142. *See id.* at 2.

"deep" and "broad"[143] tracking that would result from the merger would likely reduce the quality of the search engine product for consumers with "high privacy preferences."[144] The FTC ultimately approved Google's merger with DoubleClick, and responding to the privacy concerns noted: "[T]he consumer privacy issues presented . . . are not unique to Google and DoubleClick. To the contrary, these issues extend to the entire online advertising marketplace."[145] Despite the FTC's statement, some commentators such as Senator Warren, among others, argue that when fewer companies compete in the digital marketplace, companies have less incentive to compete in key areas like protecting privacy.[146] The problem with this characterization is that it suggests concentration causes weak privacy protections. But, like the FTC pointed out back in 2007, all firms operating within the Internet ecosystem benefit from weak privacy protections.

Since then, the landscape has not changed—commercial use of consumer data remains unregulated. The FTC acknowledged this at the time saying, "we take these consumer privacy issues very seriously," and recognizing that while "such issues may present important policy questions for the Nation, the sole purpose of federal antitrust review . . . is to identify and remedy . . . harm to competition."[147] Another example clarifies this point: If Facebook divested itself of prior acquisitions WhatsApp and Instagram, it would still be advantageous for Facebook to operate under the same business model that led to the Cambridge Analytica scandal of 2018.[148]

IV. AMEND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

So far, this Note has demonstrated that antitrust enforcement is not a viable method for addressing many of the consumer harms associated with the power of Big Tech, particularly consumer exploitation and manipulation and privacy violations. It has also demonstrated that concerns about data practices online and offline are not baseless. However, ultimately, harms occurring in the Internet ecosystem are due to a lack of regulation covering the collection and use of consumer data in the commercial context. Harms are further aggravated by two factors: (1) the complexity of relationships between consumers, digital platforms, and third-party agents participating in the

143. *See* Peter P. Swire, *Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall*, EUR. PARLIMENT 5 (Oct. 18, 2007), https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/testimony_peterswire_/Testimony_peterswire_en.pdf [https://perma.cc/UX3S-2HVC] (commenting that Google has deep knowledge about the users of its products and DoubleClick would add information about consumers across a broad swath of the Internet).

144. *See id.* Swire ultimately sees the privacy issue as a *quality* issue.

145. FTC Statement on Google/DoubleClick, *supra* note 141, at 2.

146. *See* Warren, *supra* note 75.

147. FTC Statement on Google/DoubleClick, *supra* note 141, at 2.

148. *See* Len Sherman, *Why Facebook Will Never Change Its Business Model*, FORBES (Apr. 16, 2018), https://www.forbes.com/sites/lensherman/2018/04/16/why-facebook-will-never-change-its-business-model/#7e97049064a7. [https://perma.cc/E2KY-3Q9E].

collection and use of consumer data and (2) the dynamism of technological innovation. The nature of the Internet ecosystem requires more than simple legislation, which would be ill-suited to keep pace with industries that are constantly changing. Accordingly, this Note proposes Congress amend the FTC Act to expand FTC authority to enforce against practices that are unfair and deceptive to the reasonable expectations of an ordinary consumer and thereby pressuring firms to abide by those reasonable expectations.

A. The FTC's Expertise

The FTC has a broad mandate to protect consumers from unfair and deceptive practices in the marketplace, pursue law enforcement orders to stop illegal activity, and "educat[e] consumers and businesses about their rights and responsibilities."[149] It is also the nation's leader in protecting consumer privacy through this mandate and through its rulemaking authority in some narrow areas such as children's privacy, financial data security, and credit reporting.[150] As of today, it lacks rulemaking authority for consumer privacy and data security in general, but it has knowledge and expertise in these areas.[151] No other agency is as invested in bridging the divide between consumer and business interests, nor does another agency have comparable capacity to study and understand consumer and business relations as they exist today and in such diverse sectors of the economy.[152]

B. Expand FTC Authority to Enforce Against Section 5 Violations

Section 5 of the FTC Act empowers the FTC "to prevent persons, partnerships, or corporations . . . from using unfair and deceptive acts or practices in or affecting commerce."[153] Congress should amend the existing statute and empower the FTC "to prevent persons, partnerships, or corporations . . . from using unfair and deceptive acts or practices in or affecting commerce *and, with respect to consumer privacy, as understood by the reasonable expectations of an ordinary consumer*." The FTC should then shape its policy to further define the "reasonable expectations of an ordinary consumer" through the analysis of data collected by its Consumer Sentinel complaint database. The changes to Section 5 will have a number of important effects on the kinds of behaviors the FTC can enforce against and its success in suing to mitigate consumer harms while continuing to allow the digital marketplace to self-regulate and evolve over time.

---

149. *Oversight of the Federal Trade Commission: Hearing Before the S. Subcomm. on Consumer Prot., Prod. Safety, Ins., and Data Sec. of the Comm. On Commerce, Science, and Transportation*, 115th Cong., 2nd Sess., 3 (2018) (testimony of Fed. Trade Comm'n).

150. *Id.* at n.20.

151. *Id.* at 7.

152. *See About the FTC*, https://www.ftc.gov/about-ftc (last visited Nov. 17, 2020) [https://perma.cc/D3F2-N7PG].

153. 15 U.S.C. § 45(a)(1)–(2).

By allowing the FTC to bring actions according to actual consumer expectations, the law would fill a gap that currently exists in the absence of federal privacy legislation. The FTC can stop unfair and deceptive practices in the handling of consumer data, but the scope of its enforcement is severely restricted by its mandate, which limits its enforcement power in circumstances where a business does not have a privacy policy or where the business's acts did not violate its privacy policy.[154]

Amending the FTC Act to protect consumer expectations of privacy fits within the FTC's evolving privacy role, which has already been expanded through the Gramm-Leach-Bliley Act[155] (GLBA) and the Children's Online Privacy Act (COPPA).[156] Even still, the power of the FTC to enforce consumer privacy protections follows the self-regulatory approach thus far embraced in the U.S., where "businesses essentially determine for themselves the basic rules they will adhere to regarding data collection, use, and disclosure."[157]

The amendment will follow in this spirit and allow the relationship between the FTC, businesses, and consumers to continue to evolve in the same fashion. The only change will be that consumers' consensus understanding of reasonable privacy expectations will be the baseline for determining an unfair and deceptive practice regarding data collection and use. Ultimately, this change will work to reign in the general attitude embraced by the Internet's business community, which is generally, *collect data at all costs and in whatever ways possible and worry about the consequences later*. The new law will slow companies down. It will force them to find ways to effectively communicate and educate their consumers on their data collection practices. Ultimately, it will force companies to put customer interests at the forefront of their decision-making process.

This law does not automatically swing the enforcement pendulum in the consumers' favor. Because it is based on the "reasonable expectations of an ordinary consumer," it is flexible enough to distinguish the contours of what people actually know, what people are expected to know, and what would be a genuine surprise to an ordinary consumer. Additionally, the law is flexible enough to adapt to changes in the marketplace. As business

---

154. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COL. L. REV. 583, 599 (2014) ("Because the FTC could only enforce FTC Act violations or infringements of other laws that granted it regulatory authority and because the FTC lacked the ability to enact substantive privacy rules of its own, if a company not regulated by such a jurisdiction-granting statute lacked a privacy policy, then the FTC would have nothing to enforce. Thus, the FTC appeared to be limited to enforcing whatever a company promised, and most companies were under no obligation to make any promises to restrict their collection and use of personal data.").

155. The GLBA covers consumer financial data.

156. *See* Solove & Hartzog, *supra* note 154, at 599–604 ("[B]etween 1995 and 2000, the FTC jumped into the privacy regulatory space in a dramatic way, acquiring new power with each passing year. As the FTC began to enforce COPPA and GLBA, it largely followed the same model as the notice-and-choice regime it relied upon to enforce its general Section 5 powers.").

157. *Id.* at 604 (noting that "FTC enforcement added some teeth to the promises in privacy policies, most of which lacked any penalty or consequence if a company failed to live up to its promises.").

practices evolve to meet consumer expectations and businesses become more adept at communicating practices, the law will adapt along with them.

Under the proposed amendment, the FTC will inform itself of the reasonable expectations of an ordinary consumer and base decisions on information found in its Consumer Sentinel, which contains rich data about the problems consumers face in the digital marketplace.[158] The FTC already uses the database to "spot trends, identify questionable business practices and targets, and enforce the law."[159] In 2019, "Sentinel received over 3.2 million consumer reports" through the FTC call center and from complaints filed online.[160] Every year, the FTC aggregates the information collected through Sentinel into an interactive report and compiles it alongside reports filed from "other federal, state, local, and international law enforcement agencies, as well as other organizations like the Better Business Bureau and Publishers Clearing House."[161] Through Sentinel, the FTC has data analytics expertise that will enable it to correctly identify the pain points between consumer expectations and business practices while also avoiding abuses such as false or misleading complaints. Sentinel will serve as a reference supplement for determining whether enforcement action is needed under the amended law.

C. Expand FTC Authority to Order Conduct

In bringing enforcement actions against unfair and deceptive practices, the FTC issues orders to stop entities from further engaging in a practice.[162] Accordingly, the FTC opens a proceeding that allows the accused to offer a defense.[163] If the FTC finds the defense inadequate, it can proceed to "issue . . . an order requiring such [entity] to cease and desist from using . . . such act or practice" appealable in the U.S. Courts of Appeals.[164] To ensure the FTC is fully empowered to enforce orders in the interest of the reasonable expectations of ordinary consumers, Congress must amend Section 5 of the FTC Act to read, "if upon such hearing the [FTC] shall be of the opinion that . . . the act or practice in question is prohibited . . . [it] shall issue . . . an order requiring such [entity] to cease and desist from using . . . such act or practice *and, with regard to consumer privacy, in accordance with the reasonable expectation of an ordinary consumer*."

In issuing orders, the FTC provides wrongdoers with remedial steps to comply with an order but cannot order measures that are too vague for a

158. *See* FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK, DATA BOOK 2019 2 (Jan. 2020), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf [https://perma.cc/W28H-CT34].

159. *Id.*

160. *Id.*

161. *Id.*

162. 15 U.S.C. § 45(b).

163. *See id.*

164. *Id.*

company to determine acts required for compliance.[165] By adding the above language to the statute, the FTC will be able to offer companies and courts sufficient clarity on the standards for what is required under an order. While it is important that orders are not too vague, most orders are issued according to settlements.[166] In those situations, the FTC and parties have the opportunity to negotiate the contours of how a company must proceed.[167] Therefore, this amendment will function to inform relevant actors of the contents of settlements and the acts necessary to comply.

Section 5 also authorizes the FTC to "reopen and alter, modify, or set aside, in whole or in part any report or order . . . whenever in the opinion of the [FTC] conditions of fact or of law have so changed as to require such action or if in the public interest shall so require. . . ."[168] The FTC may initiate these actions or do so at the request of parties subject to an order.[169] This provision of the statute provides flexibility in the reevaluation of orders in light of the Internet ecosystem's dynamism. Altogether, the process accommodates the diversity of interests that come together under Section 5 enforcement. It is strong enough to stop obvious bad actors and supple enough to offer solutions that maximize the interests of different parties. Overall, amending the FTC Act is the best path forward to guard against consumer exploitation, manipulation, and privacy violations occurring in the Internet ecosystem.

For over 100 years, the FTC has cultivated expertise in the area of consumer protection. This talent and skill set should not go to waste. The infrastructure needed to rebuild trust between consumers and business in the digital marketplace is, for the most part, in place. It is simply a matter of slightly retooling the capacity of the FTC, which this proposal does, in order to move the marketplace in the right direction.

VI. CONCLUSION

In 1997, the time of early commercial Internet, some of the Internet's original architects warned "[t]he most pressing question for the future of the Internet is not how the technology will change, but how the process of change

165. *See* LabMD, Inc v. Fed. Trade Comm'n*,* 894 F.3d 1221, 1237 (11th Cir. 2018) (striking down an FTC order which gave a company standards to follow to craft a reasonable security program because the approach was too broad and would make it difficult for a reviewing court to determine if the company had complied with the order).

166. Deborah L. Feinstein, Director, FTC Bureau of Competition, Remarks at GCR Live on The Significance of Consent Orders in the Federal Trade Commission's Competition Enforcement Efforts (September 17, 2013) 2 (transcript available at https://www.ftc.gov/sites/default/files/documents/public_statements/significance-consent-orders-federal-trade-commission%E2%80%99s-competition-enforcement-efforts-gcr-live/130917gcrspeech.pdf [https://perma.cc/5RD4-ZQKG]).

167. *See id.* at 5.

168. 15. U.S.C. § 45(b).

169. *Id.*

and evolution itself will be managed."[170] More than two decades later, America still grapples with this question. The Internet ecosystem is a complex network of relationships, and however concentrated it may appear to be, Congress and regulators must take a closer look. Big Tech's spectacular size is not the root of consumer harm online. If regulators break up Big Tech, dysfunction will still persist.

Unlike breaking up Big Tech, this Note's proposed amendments to Section 5 of the FTC Act would help rectify harms online. It would quell imbalances caused by self-regulation of data collection and data use practices. Seeking to fix these harms through the flexibility of Section 5 of the FTC Act would preserve fast, dynamic evolution of the commercial Internet while also offering protection to consumers. This change would accommodate the interest of consumers and businesses alike while also providing needed legislative relief in an area ignored for too long.

170. Barry M. Leiner et al., *A Brief History of the Internet*, INTERNET SOC'Y 17 (1997), https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf [https://perma.cc/UQ2N-SG25].

If a Picture Is Worth a Thousand Words, Your Mugshot Will Cost You Much More: An Argument for Federal Regulation of Mugshots

Brooke Rink*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School; B.A., International Affairs and French, Florida State University. Thank you to the staff of the Federal Communications Law Journal for their contribution and assistance with publication. I would also like to thank my family and wonderful partner Andrew for their unconditional love and support.

I. INTRODUCTION

For over a year, Jesse T., of Sonoma County, California, unsuccessfully applied for a number of jobs, from construction to electrical positions.[1] Knowing something was amiss, Jesse decided to search his name on Google.[2] The top search result was a post on Mugshots.com, which is a website that submits freedom of information requests and searches online databases to obtain criminal records.[3] Even though Jesse was never convicted of any charge, Mugshots.com still posted his booking photo along with his full name, address, and information regarding his arrest.[4] The only way to remove his mugshot from the website was to pay $399.[5] In fact, the $399 unpublishing fee was *per charge*.[6]

Mugshots.com is not the only website that publishes booking photos. Other sites include Busted Newspaper, Arrests.org, Florida.arrests.org, and Phoenixmugs.com, among many others.[7] It is not uncommon for a person to pay the unpublishing fee on one website, only for the person's mugshot to pop up on another, a problem that has been compared to a game of "whack-a-mole."[8] A person can spend thousands of dollars before realizing it is a scam.[9] Although some people can afford a lawyer to help take their mugshots down, most of those arrested cannot.[10]

Because there were over 10.3 million arrests in the United States in 2018 alone, companies like Mugshots.com impact a large portion of our population.[11] One in three Americans eligible for employment have some sort of criminal record, including arrests not resulting in a conviction.[12] These websites "humiliate their subjects . . . because mugshots create a powerful

---

1. Samantha Schmidt, *Owners of Mugshots.com Accused of Extortion: They Attempted 'to Profit Off of Someone Else's Humiliation*,' CHI. TRIB. (May 18, 2018), https://www.chicagotribune.com/business/ct-biz-mugshot-website-owners-extortion-20180518-story.html [https://perma.cc/2FN3-YXR3].
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. Olivia Solon, *Haunted by a Mugshot: How Predatory Websites Exploit the Shame of Arrest*, GUARDIAN (June 12, 2018, 3:01 PM), https://www.theguardian.com/technology/2018/jun/12/mugshot-exploitation-websites-arrests-shame [https://perma.cc/4UEG-79C2].
7. *Id.*
8. *Id.*
9. *Id.*
10. *Id.*
11. Erin Duffin, *USA – Number of Arrests for All Offenses 1990-2018*, STATISTA (Oct. 10, 2019), https://www.statista.com/statistics/191261/number-of-arrests-for-all-offenses-in-the-us-since-1990/ [https://perma.cc/AJ2W-VSRU].
12. Katie Rose Quandt, *Pennsylvania County Owes $67 Million After Man Finds Arrest Records on Mugshots.com*, APPEAL (Aug. 27, 2019), https://theappeal.org/pennsylvania-county-owes-67-million-after-man-finds-arrest-records-on-mugshots-com/ [https://perma.cc/6KKW-M2UK].

visual association between the subject and criminal activity, regardless of guilt."[13] In fact, courts are unlikely to show juries defendants' mugshots because the familiarity of mugshots from media leads to "the inference that the person involved has a criminal record, or has at least been in trouble with the police."[14] According to the New York Civil Liberties Union, the consequences of having a mugshot taken can affect a person for years "after an arrest, no matter how a charge was resolved, and to no discernable public benefit, [it] can impact the subject's personal and romantic life, child custody, job prospects, college or other educational opportunities, rental or license applications, and career advancement."[15] Indeed, some states even automatically disqualify individuals with certain criminal records from obtaining professional licenses, such as roofing and barbering.[16]

Furthermore, the posting of mugshots online is especially a problem for those who have their records sealed or expunged. Six states passed "clean slate" statutes that automatically seal eligible criminal records.[17] Although well-intended, these statutes are ineffective if an employer can still find your mugshot with a quick Google search. Expungement and record sealing allow individuals to withhold from employers the fact that they have a record; however, after a Google search, the employer will be able to find the mugshot and then will conclude the person is "a liar and a criminal."[18]

Companies like Mugshots.com are not the only ones profiting off public access to mugshots. "[R]eputation management firms, mugshot removal services, media companies that publish mugshot galleries and search engines like Google" all benefit from the further humiliation of a significant part of our population.[19] This exploitive mugshot industry has generated several lawsuits and has caused elected officials to rethink classifying mugshots as public records.[20] As a result, mugshot websites have switched from charging takedown fees to selling "reputation management services."[21] They also rely on advertising revenue from those who visit these sites.[22] In addition,

13. Solon, *supra* note 6 ("The [criminal] association is deemed so powerful that courts try to avoid showing mugshots to juries to avoid prejudice.").

14. Barnes v. United States, 365 F.2d 509, 510–11 (D.C. Cir. 1966).

15. *Legislative Memo: "Mugshot" and Booking Information Ban,* N.Y. CIVIL LIBERTIES UNION, https://www.nyclu.org/en/legislation/legislative-memo-mugshot-and-booking-information-ban (last visited Nov. 19, 2019) [https://perma.cc/TZV2-HHLF].

16. Quandt, *supra* note 12.

17. *See id.*

18. *Id.* (quoting Daryoush Taha).

19. Solon, *supra* note 6.

20. Sarah Esther Lageson, *It's Time for the Mug-Shot Digital Economy to Die*, SLATE (Mar. 12, 2019), https://slate.com/technology/2019/03/mug-shot-economy-cuomo-proposal.html [https://perma.cc/R5C9-GQGC] (N.Y. Gov. Andrew Cuomo proposed exempting mugshots from public records laws; C.A. A.G. Xavier Becerra brought criminal charges against operators of Mugshots.com for extortion, money laundering, and identity theft; a federal court found "that a Pennsylvania county violated state criminal record law by posting thousands of inmate mug shots on the local jail's website.").

21. *See id.*

22. *See id.*

Mugshots.com now displays the word "news" in its logo, which is an example of how mugshot websites are gearing up to make First Amendment arguments.[23] Local newspapers also profit from advertising revenue after posting mugshots, and these mugshots often end up on social media.[24] Although newspapers have broad First Amendment protections, it is unclear why an array of photos with zero context is considered newsworthy.

Because of how pervasive and widespread the circulation of mugshots has become—enough so that it birthed an entire industry—Congress should enact a statute that keeps up with the Internet Age. Before the Internet, a person could be arrested, acquitted, and then successfully move on with their life because arrests did not generally appear on pre-employment checks.[25] However, today, most employers Google applicants before offering them a job.[26] When a mugshot is available online indefinitely, even for those arrests which do not result in a conviction, this poses a significant hinderance to employment, housing, and interpersonal relationships.[27] Because making mugshots freely available imposes significant privacy costs and other burdens well in excess of any public benefit, Congress has, and should exercise, authority to limit the release and distribution of mugshots at both the federal and state levels. This Note will first examine federal treatment of booking photos and freedom of information requests, followed by state treatment of booking photos. Then it will offer two solutions for how Congress may address the mugshot industry: first, Congress should enact a statute prohibiting law enforcement from releasing booking photos until after a person is convicted of an offense, unless there is a compelling need to distribute a person's mugshot, such as attempting to find a fugitive; and second, Congress should carve out an exception to Section 230 of the Communications Act that would allow a plaintiff to seek equitable relief from the court in order to require search engines to remove links to websites with exploitative removal practices.

II. BACKGROUND

A. Federal Authorities Recognize the Privacy Interest in Booking Photos

Although mugshots seem engrained into our culture, their disclosure at the federal level is actually considered an "unwarranted invasion of privacy"

---

23. *Id.*
24. *Id.*
25. *See* Dan Clark, *How Many U.S. Adults Have a Criminal Record? Depends on How You Define It*, POLITIFACT (Aug. 18, 2017), https://www.politifact.com/new-york/statements/2017/aug/18/andrew-cuomo/yes-one-three-us-adults-have-criminal-record/ [https://perma.cc/T4CC-EXQ4].
26. *See* Susan P. Joyce, *What 80% of Employers Do Before Inviting You for an Interview*, HUFFPOST (May 1, 2014), https://www.huffpost.com/entry/job-search-tips_b_4834361 [https://perma.cc/LQ5F-ZSYZ].
27. *Legislative Memo*, *supra* note 15.

for the purpose of Freedom of Information Act (FOIA) requests.[28] This section will first examine the U.S. Marshals Service's (USMS) decision to prohibit disclosure under FOIA, then it will examine the federal circuit-level opinions upholding this decision. It will also examine Supreme Court decisions that focus on disclosure of criminal histories.

Congress passed FOIA in 1966 which, according to the legislative history, was designed "to permit access to official information long shielded unnecessarily from public view" and "to create a judicially enforceable public right to secure such information from possibly unwilling official hands."[29] FOIA's principal aim is government transparency. Exemption 7(C), however, prohibits disclosure of "records or information compiled for law enforcement purposes . . . to the extent that the production . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy."[30] This exemption requires courts to balance public interest in disclosure against the privacy interest Congress intended the exemption to protect.[31]

The USMS is the agency responsible for responding to FOIA requests regarding federal criminal records.[32] Beginning in 1971, the USMS adopted a nondisclosure policy for booking photos based on the assertion that disclosure would constitute an unwarranted invasion of personal privacy that exemption 7(C) sought to protect.[33]

In 1996, the Sixth Circuit held in *Detroit Free Press, Inc. v. United States Department of Justice* (*Free Press I*), that the USMS could not prevent disclosure of booking photos because criminal defendants did not have any privacy interest in the photos.[34] Thus, exemption 7(C) of FOIA does not apply.[35] Because *Free Press I* specifically dealt with individuals under indictment and awaiting trial, the Court stated that it "need not decide today whether the release of a mugshot by a government agency would constitute an invasion of privacy in situations involving dismissed charges, acquittals, or completed criminal proceedings."[36] There seems to be a certain level of skepticism about whether public access would serve any legitimate purpose in those circumstances.[37]

---

28. *See* Detroit Free Press, Inc. v. U.S. Dep't of Justice, 829 F.3d 478, 485 (6th Cir. 2016) [hereinafter *Free Press II*]; Karantsalis v. U.S. Dep't of Justice, 635 F.3d 497, 503 (11th Cir. 2011); World Publ'g Co. v. U.S. Dep't of Justice, 672 F.3d 825, 831–32 (10th Cir. 2012). Federal recognition of an important privacy interest in mugshots will serve as a backdrop for this Note's proposed legislation.

29. EPA v. Mink, 410 U.S. 73, 80–81 (1973).

30. 5 U.S.C. § 552(b)(7)(C).

31. Eumi K. Lee, *Monetizing Shame: Mugshots, Privacy, and the Right to Access*, 70 RUTGERS U. L. REV. 557, 577 (2018).

32. *Id.* at 587.

33. *Id.*

34. Detroit Free Press, Inc. v. U.S. Dep't of Justice, 73 F.3d 93, 96–97 (6th Cir. 1996).

35. *Id.*

36. *Id.* at 97.

37. *See id.* at 98 (finding that public disclosure of mugshots can serve the purpose of government oversight "in limited circumstances," such as incidents where the government detains the wrong person or in cases of police brutality).

Twenty years later, the Sixth Circuit recognized *Free Press I* as untenable because of the accessibility of mugshots online: "In 1996, this court could not have known or expected that a booking photo could haunt the depicted individual for decades. Experience has taught us otherwise."[38] Relying on Supreme Court precedent, it stated that exemption 7(C) needs to be understood "in light of the consequences that would follow from unlimited disclosure."[39] Because courts also consider "potential derivative uses" of the information sought,[40] the Sixth Circuit recognized the damaging personal consequences of mugshot websites and the "online-reputation-management industry."[41] A concurring judge found the dissemination of the photos "for malevolent purposes" problematic and stated that "these images preserve the indignity of a deprivation of liberty, often at the (literal) expense of the most vulnerable among us."[42] The court also agreed with the USMS's case-by-case approach to the release of booking photos.[43] Under this approach, the public's interest must be within the scope of the core purpose of FOIA: government transparency.[44]

Between *Free Press I* and *Free Press II*, two other circuit courts decided the question of whether booking photos constituted an unwarranted invasion of privacy. In 2011, the Eleventh Circuit stated that a booking photo "is a unique and powerful type of photograph" that creates an association of guilt and depicts the individual in a "vulnerable and embarrassing" state.[45] Thus, it found that there is a substantial personal privacy interest at stake and that disclosing booking photos does not serve any public interest that FOIA was designed to protect.[46] The court rejected the argument that general curiosity was sufficient to justify disclosure because it "is not a cognizable interest that would contribute significantly to public understanding of the operations or activities of the government."[47] In 2012, the Tenth Circuit reached the same conclusion, citing the Eleventh Circuit's decision with approval.[48] Therefore, all three circuit courts concluded that individuals enjoy a substantial privacy interest in their booking photos that is not outweighed by any public interest.

Furthermore, all three circuits relied on the Supreme Court's decision in *United States Department of Justice v. Reporters Committee for Freedom*

38. *Free Press II*, 829 F.3d at 485 ("Today, an idle internet search reveals the same booking photo that once would have required a trip to the local library's microfiche section.").
39. *Id.* at 482 (citing Nat'l Archives & Recs. Admin. v. Favish, 541 U.S. 157 (2004)).
40. *Id.* (citing Am. Civ. Liberties Union v. U.S. Dep't of Justice, 655 F.3d 1, 7 (D.C. Cir. 2011)).
41. *Id.* at 482–83.
42. *Id.* at 486.
43. *Id.* at 485.
44. *See id.*
45. *Karantsalis*, 635 F.3d at 503.
46. *See id*. at 503–04.
47. *Id.* (citing U.S. Dep't of Justice v. Reps. Comm. for Freedom of Press, 489 U.S. 749 (1989)).
48. *World Publ'g Co*., 672 F.3d at 829 (concluding that disclosure of booking photos would not contribute to public understanding of federal law enforcement).

of Press, which held that the disclosure of rap sheets compiled by the Federal Bureau of Investigation (FBI) constitutes an unwarranted invasion of privacy, therefore falling under exemption 7(C) of FOIA.[49] Rap sheets include "descriptive information, such as date of birth and physical characteristics, as well as a history of arrests, charges, convictions, and incarcerations of the subject."[50] The Court began its analysis by balancing the privacy interest at stake against public interest in disclosure.[51] It rejected the "cramped" argument that there is no privacy interest in rap sheets because they only contain information already available to the public.[52] Instead, it defined privacy as an individual's ability to control information "concerning his or her person."[53] The FBI spends resources to compile and maintain rap sheets, which demonstrates that the information is not freely available to the public or to the officials who have access to them.[54] The Court found a "vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[55]

Additionally, the Court found support in its conclusion from FOIA and the Privacy Act of 1974.[56] The legislative intent behind FOIA was not to disclose personal details about private citizens, but to allow the public access to activities of the government.[57] The Privacy Act was intended to mitigate "the impact of computer data banks on individual privacy."[58]

Further, the Court found significance in states' decisions to prohibit access to non-conviction data in criminal records.[59] Given the level of concern Congress and the states had expressed at the time, it concluded that "individual subjects have a significant privacy interest in their criminal histories."[60] That interest is compounded by the reality that a computer can "store information that would otherwise surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded."[61] The Court concluded that when the subject of a rap sheet is a private citizen, the privacy interest is "at its apex while the FOIA-based public interest in disclosure is at its nadir."[62]

---

49. 489 U.S. 749 (1989).
50. *Id.* at 752.
51. *See id.* at 762.
52. *See id.* at 762–63.
53. *Id.* at 763.
54. *See id.* at 764.
55. *Id.*
56. *Id.* at 765–66.
57. *See id.*
58. *Id.* at 766 (citing H.R. REP. NO. 93-1416, at 7 (1974)).
59. *Id.* at 767.
60. *Id.*
61. *Id.* at 771.
62. *Id.* at 780.

Although the Court accepts that there is no FOIA-based public interest in the disclosure of rap sheets, it has not recognized due process protection for mugshot distribution.[63] In *Paul v. Davis*, a 1976 case, the Court seemed to suggest that distribution of the plaintiff's mugshot before his conviction would better support a claim for defamation than it would for a procedural due process violation.[64] Justice William Brennan issued a strong dissent to this opinion:

> The Court today holds that police officials, acting in their official capacities as law enforcers, may on their own initiative and without trial constitutionally condemn innocent individuals as criminals and thereby brand them with one of the most stigmatizing and debilitating labels in our society. If there are no constitutional restraints on such oppressive behavior, the safeguards constitutionally accorded an accused in a criminal trial are rendered a sham . . . The Court accomplishes this result by excluding a person's interest in his good name and reputation from all constitutional protection, regardless of the character or necessity for the government's actions. The result, which is demonstrably inconsistent with prior case law and unduly restrictive in its construction of our precious Bill of Rights, is one in which I cannot concur.[65]

Justice Brennan recognized the "debilitating" effect a mugshot can have on an individual, even though this case was decided long before a person's mugshot became the top search result after an Internet search of their name.[66] The notion that one is innocent before proven guilty is a legal fiction if the government can distribute a person's mugshot before conviction.[67]

In summary, federal courts have no difficulty finding a substantial privacy interest in booking photos and criminal histories in general when weighed against the FOIA-based public interest in disclosure. Further, the increased accessibility and longevity of these records due to the Internet seems to weigh heavily on the courts as well as Congress. Although Congress and the courts have recognized an important privacy interest in booking photos, existing protections are insufficient because they give the government too much discretion to voluntarily release booking photos even when release is not mandated.

63. *See* Paul v. Davis, 424 U.S. 693, 697–98 (1976) (rejecting plaintiff's procedural due process claim because damage to reputation is insufficient).

64. *See id.*

65. *Id*. at 714 (Brennan, J., dissenting).

66. *See id.*

67. *See id.*

B. States' Treatment of Booking Photos

The previous section discussed federal treatment of booking photos, but criminal law primarily comes from decisions of state and local governments. Federal recognition of a privacy interest in booking photos is encouraging, but it is state treatment that likely has a greater impact on our population. This section will begin by examining the early state case law regarding booking photos, then it will discuss the case law following the passage of FOIA and the states' FOIA equivalents. Finally, it will assess states' reactions to the emergence of websites such as Mugshots.com.

State courts began grappling with booking photos as early as 1899, when cameras were relatively new.[68] In New York, a court held that the police have the right to photograph habitual criminals and to distribute those photos in certain ways.[69] However, the opinion suggested that if a person had been incorrectly labeled a criminal and had his photo distributed, he would have a claim for libel against the police.[70]

In 1905, a man brought a right of privacy claim against the police for distributing his mugshot after his arrest.[71] The Louisiana court decided that sharing his mugshot was improper because he was not a "hardened criminal."[72] Even though he was arrested a number of times before this incident, the court stated that "before conviction his picture should not be posted, for then it would be a permanent proof of [his] dishonesty."[73]

Subsequently, several other state courts followed suit; each recognized a privacy interest that exists in mugshots, especially in light of the lasting reputational harm a mugshot can have.[74] This recognition quickly ceased when FOIA and the states' FOIA equivalents passed into law in the 1960s.[75] State laws were broadly interpreted as allowing public access to a wide range of government information, including mugshots.[76] Thus, whether mugshots are a matter of public record largely depends on the state's statute and whether mugshots fall within any statutory exemption.[77]

---

68. *See* Amy Gajda, *Mugshots and the Press-Privacy Dilemma*, 93 TUL. L. REV. 1199, 1206–07 (2019).

69. People ex rel. Joyce v. York, 59 N.Y.S. 418 (N.Y. Sup. Ct. 1899).

70. *See id.*

71. Itzkovitch v. Whitaker, 42 So. 228, 229 (La. 1906).

72. *See id.*

73. *Id.*

74. *See* Gajda, *supra* note 68, at 1209 (citing McGovern v. Van Riper, 43 A.2d 514, 525 (N.J. Ch. 1945) ("[U]nless an accused becomes a fugitive from justice there exists no right to publish or disseminate his . . . photographs . . . in advance of conviction"); State ex rel. Mavity v. Tyndall, 66 N.E. 2d 755, 761–63 (Ind. 1946) (warning there may be exceptional cases that warrant destruction of mugshots; those cases should be decided by balancing right of privacy against public interest); *see also* Bingham v. Gaynor, 126 N.Y.S. 353, 357 (N.Y. App. Div. 1910) (stating a person could be "ruined for life" and "he and his parents have lived in daily dread of the day his employer would learn that his picture is in the 'Rogues' Gallery")).

75. Gajda, *supra* note 68, at 1209–10.

76. *Id.*

77. Lee, *supra* note 31, at 591–92.

A majority of states—approximately thirty—consider mugshots to be a matter of public record.[78] Some of these states explicitly provide for the release of mugshots, such as Virginia, North Dakota, Minnesota, and Nebraska.[79] In other states, courts or agencies interpret the statutes as allowing the distribution of mugshots.[80]

Georgia, Kansas, Montana, New Jersey, and Washington consider mugshots exempt from public disclosure.[81] In Montana, mugshots are considered confidential, and public disclosure is only allowed "upon a written finding that the demands of individual privacy do not clearly exceed the merits of public disclosure."[82] Further, if an arrest does not result in a conviction, all photographs and fingerprints taken must be returned to the individual.[83]

The remaining states do not have a "clear authority from the judicial or executive branch" which would determine if mugshots fall within the state's public records statute.[84] Some states have a balancing approach that weighs the invasion of privacy against public interest in disclosure.[85] In California, former Attorney General Bill Lockyer gave discretion to law enforcement agencies to decide whether or not to release mugshots, which resulted in varying practices across the state.[86]

Most recently, states contend with the problem of the exploitative nature of the mugshot industry emerging online. For instance, New York Governor Andrew Cuomo proposed a ban on the release of mugshots in 2019.[87] A spokesman for Cuomo stated the proposal is designed "to help curtail an unethical practice that amounts to extortion of formerly incarcerated individuals."[88] He also highlighted that fifteen other states "passed legislation that prohibits websites from charging fees for removing photos" and that it "is not working—mugshots keep popping up online."[89]

78. *Id.* at 593.

79. *Id.* (Virginia has exception where release would jeopardize an ongoing investigation).

80. *Id.* at 593–94 (Attorneys General from Alabama, Florida, Maryland, and Oklahoma interpreted public records statutes as allowing disclosure of mugshots; a Wisconsin court of appeals held that a mugshot was a "record" for the purpose of the state's public records law).

81. *Id.* at 594.

82. *Id.* at 595.

83. *Id.*

84. *Id.* at 596.

85. *Id.*

86. *Id.* at 597.

87. Brendan J. Lyons, *Cuomo Proposes Ban on Release of Mugshots, Arrest Info*, TIMESUNION (Jan. 20, 2019, 6:38 PM EDT), https://www.timesunion.com/news/article/Cuomo-proposes-ban-on-release-of-mugshots-arrest-13545073.php [https://perma.cc/93HL-FZ5Q].

88. *Id.*

89. *Id.*

In addition, a handful of states passed legislation allowing for the automatic sealing of eligible criminal records.[90] In 2018, Pennsylvania became the first state to pass "clean slate" legislation, followed by Utah.[91] Further, Arkansas and California are considering passing their own clean slate statutes.[92] Pennsylvania's clean slate law allows 30 million criminal cases to be sealed "so that they cannot affect people's chances for employment, education and housing."[93] Although well-intended, if mugshots are still released to the public and uploaded to the Internet, employers, landlords, and educational institutions will still likely judge a person based on their mugshot.[94]

Overall, state courts have recognized the privacy interest at stake in mugshots since the beginning of the 20th century. Courts seem to struggle with the lasting reputational harm caused by the distribution of a mugshot before a person is convicted. Further, recent legislation enacted by states demonstrates an increased intolerance of the exploitation of people with criminal records. It is also an acknowledgement that there is no societal benefit to websites that simply post mugshots with no follow-up on the final disposition of those cases. New York in particular has recognized that as long as mugshots are available to the public, this problem will always exist. If an employer or landlord can still access a person's mugshot online, record sealing will not be of much use.

III. ANALYSIS

A. Congress Should Enact a Law Prohibiting the Distribution of Booking Photos Until After a Person is Convicted

As long as mugshots remain easily accessible by the public, the exploitative mugshot industry will continue to exist. As previously discussed, the consequences of classifying mugshots as public record, which has devastating and lasting implications for those depicted, far outweigh any public interest in disclosure. Whether a person will be haunted by their mugshot arbitrarily varies based on the policy choices of each state. Because employers, landlords, and educational institutions frequently Google their applicants, a mugshot can significantly diminish a person's potential to earn income.[95] This reality is equally true for both convicted persons and for

90. Hannah Knowles, *Criminal Records Can Be a 'Life Sentence to Poverty.' This State is Automatically Sealing Some*, WASH. POST (July 1, 2019), https://www.washingtonpost.com/nation/2019/07/01/criminal-records-can-be-life-sentence-poverty-this-state-is-automatically-sealing-some/ [https://perma.cc/S3GW-9T26].

91. *Id.*

92. *Id.*

93. *Id.*

94. Quandt, *supra* note 12 (quoting Daryoush Taha).

95. Knowles, *supra* note 90 ("even a minor offense can be 'a life sentence to poverty," and University of Michigan researchers stated individuals who expunged their records "saw their wages go up by more than 20 percent within a year").

persons acquitted or even wrongly accused. If there are no restraints on the release of mugshots, as Justice Brennan wrote, the safeguards of the Constitution "in a criminal trial are rendered a sham."[96] Thus, Congress should enact a statute that prohibits the distribution of mugshots until a person is convicted of a crime. This statute would protect the innocent from the hot iron branding of "one of the most stigmatizing and debilitating labels in our society."[97] This section will first examine the public interest in the publication of mugshots. It will then argue that distribution of mugshots into interstate commerce provides the hook necessary to support federal regulation.[98]

There is little societal benefit to publishing millions of mugshots online beyond morbid curiosity. Proponents of disclosure argue that it provides insight into the criminal justice system and that it allows for greater accountability. However, the Sixth, Tenth, and Eleventh Circuits rejected that exact argument: mugshots do not contribute to "public understanding of the operations" of the government and "the public obtains no discernable interest from viewing the booking photographs, except perhaps the negligible value of satisfying voyeuristic curiosities."[99]

Mugshot galleries display the depicted individual's name, age, and suspected offense, but there is hardly ever any follow-up coverage.[100] The intent behind these galleries is not to inform; it is to ridicule.[101] As the Sixth Circuit noted, these galleries target "the most vulnerable among us."[102] Indeed, the most viral mugshots tend to display people who are clearly suffering from mental illness or addiction issues.[103] Further, some local media outlets recognize that all they need is "goofy mugshots" in order to get more clicks.[104] The notoriety of "Florida man" also demonstrates "the runaway racism and classism [that are] baked into the cake of the mugshot industry."[105] "Florida man" has become so popular that in 2019, the "Florida man challenge" emerged.[106] This "challenge" entailed googling a person's birthday, followed by the phrase "Florida man," to find a Florida arrest story that happened on that person's birthday.[107] A survey of "Florida man" headlines includes "Florida Man Killed Ex-Girlfriend While Trying to 'Get

96. 424 U.S. at 714 (Brennan, J., dissenting).
97. *Id.*
98. *See generally* Lee, *supra* note 31.
99. *Karantsalis*, 635 F.3d at 504; *see* 672 F.3d 825; *see also* 829 F.3d 478.
100. Corey Hutchins, *Mugshot Galleries Might Be a Web-Traffic Magnet. Does That Justify Publishing Them?*, COLUM. JOURNALISM REV. (Oct. 24, 2018), https://www.cjr.org/united_states_project/mugshots-ethics.php [https://perma.cc/82ZP-QZXV].
101. Adam Johnson, *The Media's Profitable, Indefensible Addiction to Mugshots*, FAIR (Jan. 23, 2019), https://fair.org/home/the-medias-profitable-indefensible-addiction-to-mugshots/ [https://perma.cc/RXS7-VBLJ].
102. *Detroit Free Press*, 829 F.3d at 486.
103. Johnson, *supra* note 101.
104. *Id.*
105. *Id.*
106. Ashley Hoffman, *The Florida Man Challenge Is a Bizarre News Bonanza*, TIME (Mar. 21, 2019), https://time.com/5555893/florida-man/ [https://perma.cc/9KRU-LWGS].
107. *Id.*

Rid of the Devil;' " "Florida Man Chews Up Police Car Seat After Cocaine Arrest;" "Florida Man Doesn't Get Straw, Attacks McDonald's Employee;" and "Florida Man Denies Syringes Found in Rectum Are His."[108] It is easy to tie these headlines to disturbed individuals who are likely suffering from mental illness, drug addiction, and poverty.

One journalist describes mugshot galleries as "preying on human suffering" and feels that they are "the wrong way to get traffic."[109] Unfortunately, this practice will continue as long as it remains profitable.[110] According to an editor at North Carolina's *Salisbury Post*, the "Mugshot Monday" feature "is the most popular thing on the website for that particular day."[111]

On the other hand, attitudes are shifting "away from a belief that the best way to keep the public safe is to 'lock people up for as long as we could' and toward a recognition that criminal justice should be proactive about setting people up for success when they leave incarceration."[112] As Daniel Solove, privacy law professor at the George Washington University Law School, states in *The Virtues of Knowing Less*, "the benefits of rehabilitation are difficult to reject, especially in a criminal justice system from which most criminals are released back into society."[113] Solove also highlights that the possibility of rehabilitation has long been a part of American tradition.[114]

One in three Americans have some sort of criminal record, including arrests that do not result in a conviction.[115] This fact may explain the bipartisan support for initiatives such as automatic record-sealing.[116] In addition, 70% of voters support automatic record-sealing and shrinking prison

---

108. Justin Kirkland, *The 90 Wildest Florida Man Headlines of 2019 (So Far)*, ESQUIRE (Apr. 1, 2019), https://www.esquire.com/news-politics/a26899191/florida-man-headlines-2019/ [https://perma.cc/2MWC-XZ7F].

109. Hutchins, *supra* note 100.

110. *Id.* ("In 2016, Fusion looked at 74 newspapers, mostly owned by the McClatchy and Tribune Publishing chains, and found 40 percent of them published mugshot galleries online"); *see also* Ingrid Rojas & Natasha Del Toro, *Should Newspapers Make Money Off of Mugshot Galleries?*, FUSION TV (Mar. 9, 2016), https://fusion.tv/story/278341/naked-truth-newspapers-mugshot-galleries/ [https://perma.cc/PBT8-CAHK] ("[I]t appears that newspapers are monetizing police photos and public humiliation in a manner that's strikingly similar to exploitive private sites like mugshots.com").

111. Hutchins, *supra* note 100.

112. Knowles, *supra* note 90.

113. Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1057 (2003).

114. *Id.* (quoting Lawrence Fiedman) ("American society is and has been a society of extreme mobility, in every sense of the word: social, economic, geographical. Mobility has meant freedom; mobility has been an American value. People often moved from place to place; they shed an old life like a snake molting its skin. They took on new lives and new identities. They went from rags to riches, from log cabins to the White House. American culture and law put enormous emphasis on second chances.").

115. Clark, *supra* note 25.

116. Knowles, *supra* note 90 (stating Pennsylvania's Clean Slate Act was "a relatively easy sell" because it received support from "both Democrats and Republicans and garnered support well beyond defendant advocates").

populations.[117] Thus, the time is ripe for Congress to pass legislation that recognizes the public's interest in rehabilitation.

Congress previously passed privacy legislation that directly affected states' activities on multiple occasions. For instance, the Driver's Privacy Protection Act of 1994 (DPPA), codified at 18 U.S.C. §§ 2721–25, "establishes a regulatory scheme that restricts the States' ability to disclose a driver's personal information without the driver's consent."[118] Specifically, it prohibits states' departments of motor vehicles (DMVs) from "knowingly disclos[ing] or otherwise mak[ing] available to any person or entity personal information . . . about any individual obtained by the department in connection with a motor vehicle record. . . ."[119] Further, DPPA regulates "the resale and redisclosure of drivers' personal information by private persons who have obtained that information from a state DMV."[120] If a person knowingly violates DPPA, they may be subject to a criminal fine and to liability in a civil action brought by the driver.[121] If a state agency does not comply with DPPA, the United States Attorney General may impose a civil penalty of not more than $5,000 per day of substantial noncompliance.[122] Congress passed DPPA in part because "a deranged fan murdered actress Rebecca Shaeffer outside her home after acquiring [her] address from the [DMV]."[123]

In *Reno v. Condon*, the Supreme Court upheld DPPA after South Carolina challenged its constitutionality.[124] The Court ruled that DPPA is a valid exercise of Congress's authority to regulate interstate commerce under the Commerce Clause.[125] It also concluded DPPA does not violate the Tenth Amendment.[126] The Court stated that motor vehicle information "is used by insurers, manufacturers, direct marketers, and others engaged in interstate commerce."[127] The information is used by public and private entities for the purpose of interstate motoring as well.[128] The Court concluded that in this context, motor vehicle information is an article of commerce, so "its sale or release into the interstate stream of business is sufficient to support congressional regulation."[129]

---

117. *Clean Slates, Rich States – Why States Are Rushing to Seal Tens of Millions of Old Criminal Records*, ECONOMIST (Nov. 14, 2019), https://www.economist.com/united-states/2019/11/14/why-states-are-rushing-to-seal-tens-of-millions-of-old-criminal-records [https://perma.cc/UQ92-PMTS].

118. Reno v. Condon, 528 U.S. 141, 144 (2000).

119. 18 U.S.C. § 2721(a)(1) (2018).

120. 528 U.S. at 146.

121. *Id.* at 146–47 (citing 18 U.S.C. §§ 2723(a), 2724, 2725(2)).

122. *Id.* at 147 (citing 18 U.S.C. § 2723(b)).

123. Solove, *supra* note 113, at 1012.

124. 528 U.S. at 151.

125. *Id.*

126. *Id.*

127. *Id.* at 148.

128. *Id.* at 149.

129. *Id.*

Turning to the question of whether DPPA violated the Tenth Amendment, the Court stated that it treats the states as owners of databases and that it does not require states to enact any laws or "to assist in the enforcement of federal statutes regulating private individuals."[130] For purposes of congressional regulation, the parallel between motor vehicle information and mugshots is patent. Webpages such as mugshot websites inherently implicate interstate commerce because they involve the Internet.[131] Similar to how motor vehicle information enters the interstate stream of business, mugshots are used by mugshot websites, reputation management firms, local newspapers, and even search engines for profit.[132] Thus, mugshots are a proper subject of congressional regulation.

Although *Condon* involved South Carolina's sale of motor vehicle information, that fact alone is not dispositive.[133] The Court specifically stated the "sale or release" of the information into the interstate stream of commerce was sufficient to support congressional regulation.[134] Further, other Commerce Clause cases upholding statutes have not required the direct participation of states in the market.[135] As the Court stated in *United States v. Lopez*, Congress can regulate "the instrumentalities of interstate commerce, or persons or things in interstate commerce, even though the threat may come only from intrastate activities."[136] One could also argue that distribution of mugshots has a substantial effect on interstate commerce because a significant portion of those who have their mugshots available online have a difficult time seeking employment, housing, and educational opportunities, thus hurting the economy.[137]

Because regulating mugshots would likely pass the same Commerce Clause tests as other information privacy regulations upheld by the Supreme

130. *Id.* at 151.

131. United States v. MacEwan, 445 F.3d 237, 245–46 (3d Cir. 2006) (holding that the Internet is a "channel and instrumentality of interstate commerce" and that child pornography downloaded over the Internet is a proper subject of congressional regulation even without the proof that the image crossed state lines).

132. Solon, *supra* note 6.

133. 528 U.S. at 149.

134. *Id.* at 148.

135. *See* Shreveport Rate Cases, 234 U.S. 342 (1914); Southern Ry. Co. v. United States, 222 U.S. 20 (1911).

136. United States v. Lopez, 514 U.S. 549, 558 (1995).

137. *See Reno*, 528 U.S. at 148–89.

Court, Congress can regulate mugshots.[138] Though privacy rights are still developing, the Internet era is shifting attitudes towards protecting records from public access. Following the spirit of this attitude shift, the appropriate balance to strike for mugshots is prohibiting their release until after conviction. This way, innocent people will not be permanently harmed by mugshots revealed in a simple Google search of their name. Further, the public will still be able to access the mugshots of those who actually pose some degree of danger to society. Proposed legislation should include an exception that would allow mugshot disclosure to aid in law enforcements' attempts to locate a fugitive.

B. Congress Should Carve Out an Exception to Section 230 of the Communications Act That Would Allow Courts to Require Search Engines to Remove Links to Websites with Exploitative Removal Practices

This section proposes an effective mechanism for enforcing the prohibition of pre-conviction mugshot release discussed in Section III, particularly for those who already have their mugshots posted online. As previously noted, one in three Americans eligible for employment have some sort of criminal record, including arrests not resulting in a conviction.[139] Because mugshots are a standard part of booking procedures and states allow them to be freely accessible, millions of Americans have their mugshots posted online. The availability of mugshots online deeply impacts a person's personal and family life, as well as employment and educational opportunities.[140] People should be able to request that search engines remove links to websites that require fees to remove mugshots due to the severe consequences involved.

Currently, under Section 230 of the Communications Act, search engines like Google receive immunity from being treated as publishers of third party content.[141] This section will focus on why Congress should carve out an exception to Section 230 that would allow plaintiffs to seek equitable relief in court to remove search engine links to websites with exploitative mugshot removal practices. This section will first examine Section 230,

138. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 37–38 (6th ed. 2018) ("Fair Credit Reporting Act of 1970, Pub. L. No. 90-32, 15 U.S.C. §§ 1681 et seq. – provides citizens with rights regarding the use and disclosure of their personal information by credit reporting agencies; Privacy Act of 1974, Pub. L. No. 93-579, 5 U.S.C. § 552a – provides individuals with a number of rights concerning their personal information maintained in government record systems . . . Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 20 U.S.C. §§ 1221 n.1232g – protects the privacy of school records; Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 47 U.S.C. § 551 – mandates privacy protection for records maintained by cable companies; Children's Online Privacy Protection Act of 1998, Pub. L. No. 106-170, 15 U.S.C. §§ 6501-6506 – restricts the use of information gathered from children under age 13 by Internet websites").

139. Clark, *supra* note 25.

140. *Legislative Memo*, *supra* note 15.

141. 47 U.S.C. § 230(c)(1) [hereinafter Section 230].

including its legislative history and purpose. It will then discuss the circuit split regarding its interpretation. Finally, this section will argue why the Digital Millennium Copyright Act's notice system should be incorporated into Section 230, requiring search engines to remove links to websites with exploitative removal practices.

To begin, it is necessary to understand the distinction between publishers and distributors. Publishers, such as newspapers, are responsible for content appearing on their platforms because they exert editorial control over the content.[142] In other words, publishers decide what information appears on their platforms. To hold a publisher liable for a privacy tort, one merely must show that the tortious statements in question appeared on the publisher's platform.[143] Distributors, on the other hand, solely sell or distribute third party content.[144] Examples of distributors include bookstores and newsstands.[145] A distributor is only liable for a third party's statement if it knew or should have known the statement was tortious.[146]

Two cases from the 1990s led to the enactment of Section 230.[147] In 1991, the Southern District of New York held that Internet service providers (ISPs) are distributors rather than publishers because the ISP in question had "no more editorial control over such a publication than does a public library," and it would not be feasible to require an ISP "to examine every publication it carries for potentially defamatory statements."[148] The court concluded that the ISP in question was not liable because it had no reason to know of the defamatory statements.[149] In 1995, a New York trial court drew the opposite conclusion. The computer network in question, Prodigy Services, actively screened postings for offensive material.[150] Because of Prodigy's content moderation policy, the court held that it acted as a publisher, making it liable for defamation.[151] These two conflicting cases drew the attention of then-Congressmen Christopher Cox and Ron Wyden, who believed the holding in *Stratton Oakmont* disincentivized good faith content moderation by ISPs.[152] They argued ISPs are in the best position to monitor content and that they should not be penalized for "help[ing] us control" the Internet.[153] This is the pretext to Section 230's enactment in 1996.[154]

142. Solove & Schwartz, *supra* note 138, at 176.
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.*
147. *Id.* at 177.
148. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991).
149. *Id.* at 141.
150. Stratton Oakmont, Inc. v. Prodigy Servs. Co., Trial IAS Part 34.,1995 WL 323710, at *4 (N.Y. Sup. May 24, 1995).
151. *Id.* at *4–5.
152. Andrew P. Bolson, *Flawed but Fixable: Section 230 of the Communications Decency Act at 20*, 42 RUTGERS COMPUT. & TECH. L.J. 1, 5–6 (2016).
153. 141 CONG. REC. H8468 (daily ed. Aug. 4, 1995) (statement of Rep. Christopher Cox).
154. *See* Bolson, *supra* note 152, at 5–6.

Section 230 sets out protection for "Good Samaritan" blocking of offensive material: "no provider or user of an interactive computer service shall be treated as the publisher" if a third party provides the content.[155] An interactive computer service is defined as "any information service" provider that "enables computer access by multiple users to a computer server."[156] While Section 230 immunizes interactive computer services, information content providers are not entitled to any immunity.[157] Information content providers are defined as any entity which "is responsible, in whole or in part, for the creation" of content on the Internet.[158] Thus, interactive computer services are treated similarly to distributors and information content providers are similar to publishers.

The legislative history demonstrates that Section 230 primarily intends "to balance the need to protect the safety of children with the need to allow Internet companies to grow without the fear of crippling regulation."[159] It also shows the mistaken belief held at the time that content on the Internet could be controlled with the help of companies "like the new Microsoft network."[160] Congressman Cox stated that Congress should encourage companies "to do everything possible for us, the customer, to help us control, at the portals of our computer, at the front door of our house, what comes in and what our children see. This technology is very quickly becoming available, and in fact everyone one [sic] of us will be able to tailor what we see to our own tastes."[161] That is not the case in today's Internet Age. The legislative history shows that Congress did not intend Section 230 to enable content that no one would be willing to control.[162]

To further complicate matters, the Fourth Circuit held in *Zeran v. America Online* that "publishers" and "distributors" are the same for the purpose of Section 230, despite the fact that Congress only used the word "publisher."[163] In this case, the plaintiff argued under a distributor theory of liability that Section 230 allowed liability for interactive computer services that received notice of defamatory material posted through their services and then subsequently refused to act.[164] The court rejected this argument because Section 230 "plainly immunizes computer service providers like AOL from

155. Section 230.
156. 47 U.S.C. § 230(f)(3).
157. 47 U.S.C. § 230(c).
158. 47 U.S.C. § 230(c).
159. Bolson, *supra* note 152, at 8.
160. *Id.* at 7 (citing 141 CONG. REC. H8468 (daily ed. Aug. 4, 1995) (statement of Rep. Christopher Cox)).
161. *Id.*
162. *Id.* at 8–9.
163. Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) ("once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher. The computer service provider must decide whether to publish, edit, or withdraw the posting.").
164. *Id.* at 328.

liability for information that originates with third parties."[165] This view has support in four other federal appellate courts.[166]

The Seventh Circuit, however, does not interpret Section 230(c) "as a general prohibition of civil liability" for online content hosts:[167]

> The district court held that subsection (c)(1), though phrased as a definition rather than as an immunity, also blocks civil liability when web hosts and other Internet service providers (ISPs) refrain from filtering or censoring the information of their sites . . . If this reading is sound, then § 230(c) as a whole makes ISPs indifferent to the content of information they host or transmit: whether they do (subsection (c)(2)) or do not (subsection (c)(1)) take precautions, there is no liability under either state or federal law. As precautions are costly . . . ISPs may be expected to take the do-nothing option and enjoy immunity under § 230(c)(1). Yet § 230(c)—which is, recall, part of the 'Communications Decency Act'—bears the title 'Protection for 'Good Samaritan' blocking and screening of offensive material', hardly an apt description if its principal effect is to induce ISPs to do nothing about the distribution of indecent and offensive materials via their services.[168]

The court elaborated that another possible interpretation of Section 230 is that it "forecloses any liability that depends on deeming the ISP a 'publisher'—defamation law would be a good example of such liability—while permitting the states to regulate ISPs in their capacity as [distributors]."[169] A plain language reading of Section 230 better supports this interpretation because Congress explicitly stated that interactive computer service providers will not be treated as *publishers* if the content originates from a third party.[170] It says nothing about *distributors*.[171]

---

165. *Id.*

166. Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000); Green v. Am. Online, Inc., 318 F.3d 465, 471 (3d Cir. 2003); Batzel v. Smith, 333 F.3d 1018, 1027 (9th Cir. 2003) (though the court had no need to decide whether § 230(c)(1) encompasses both publishers and distributors in the specific case. It did note that, "so far, every court to reach the issue has decided that Congress intended to immunize both distributors and publishers."); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 420 (1st Cir. 2007) ("[i]t is, by now, well established that notice of the unlawful nature of the information provided is not enough to make it the service provider's own speech").

167. Chi. Lawyers' Comm. for Civ. Rts. Under L., Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008).

168. *Id.* at 670 (citing Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003)).

169. *Id.*

170. Section 230.

171. *See id.*

The distinction matters because search engines, like Google, are interactive computer service providers under Section 230.[172] Because courts supporting the *Zeran* interpretation grant immunity for both publisher and distributor liability, plaintiffs seeking removal of their mugshots have few legal options. Therefore, Congress should, at minimum, craft an exception to Section 230 that treats search engines as distributors for the purpose of removing links to websites with exploitative removal practices. This policy fix should allow plaintiffs to seek injunctive relief from courts if, after notifying the search engine, the search engine refuses to remove the links. This notice system would be modeled after the Digital Millennium Copyright Act (DMCA), codified at 17 U.S.C. § 512.

DMCA requires service providers to remove content after receiving notice of their copyright-infringing character.[173] For search engines, the relevant provision is Section 512(d), which pertains to "information location tools."[174] It states that "information location tools" are not liable for "linking users to an online location containing infringing material" if they do not have "actual knowledge" of the material.[175] If they do not have actual knowledge, they can still be liable if they are "aware of facts or circumstances from which infringing activity is apparent."[176] Further, even after becoming aware of the infringing material, if search engines act "expeditiously" to remove the material, then they will not be liable.[177] This provision is referred to as DMCA's notice and takedown system.[178]

This notice system will also work for content that has exploitative removal practices. In fact, Google is already willing and capable of removing links to websites with exploitative removal practices in some instances.[179] For example, on a Google support webpage, it states that "upon request, under some circumstances, we may remove links to [websites that require a fee to remove content] from Google search results."[180] As Google highlights, other

172. Bennett v. Google, LLC, 882 F.3d 1163, 1167 (D.C. Cir. 2018); Parker v. Google, Inc., 422 F. Supp. 2d 492, 501 (E.D. Pa. 2006), *aff'd* 242 F. App'x 833, 838 (3d Cir. 2007).

173. 17 U.S.C. § 512 (2018).

174. H.R. REP. NO. 105-551(II), at 58 (1998); S. REP. NO. 105-190, at 49 (1998); *see also* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007) ("Google could be held contributorily liable if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10's copyrighted works, and failed such steps.").

175. 17 U.S.C. § 512(d) (2018).

176. 17 U.S.C. § 512(d)(1)(B) (2018).

177. *Id.*

178. Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 235 (2009).

179. *Remove Content about Me on Sites with Exploitative Removal Practices from Google*, GOOGLE HELP CENTER, https://support.google.com/websearch/answer/9172218 (last visited Jan. 26, 2020) [https://perma.cc/FKH2-V8AU].

180. *Id.* ("We recognize that it can be distressing when content about you is posted by others on websites. There is additional angst in discovering that you have to pay money directly to the sites or to other agencies to get the content removed").

search engine operators can still host the information, so Google's policy alone is not a true removal of the post from the Internet.[181]

A shortcoming to this approach is that it only applies to websites with exploitative removal practices and not to newspapers' mugshot galleries. Although local newspapers that publish mugshot galleries can barely be distinguished from mugshot websites, local newspapers are generally better at responding to requests for removals.[182] Some newspapers even take down mugshots after a certain period of time and prevent Google from indexing the page, thus stopping the mugshot from appearing at the top of a search result.[183] According to the Marshall Project, in February 2020, the Houston Chronicle announced that it will no longer publish mugshot galleries, joining an increasing number of media outlets that no longer tolerate this practice.[184] In response to the Houston Chronicle's decision, a spokesman for the Harris County Sheriff's Office tweeted, "I'm hopeful that other media outlets and law enforcement agencies will follow your lead and rethink the practice of publicly shaming arrested people who haven't been convicted of a crime."[185]

In sum, Congress should amend Section 230 so that search engines are required to remove links to websites with exploitative removal practices after being notified of their existence.[186] DMCA supplies an example of how that notice system should work. This proposed legislation would give practical effect to the notion of rehabilitation, as one of the worst moments in a person's life will no longer be used to exploit them.

---

181. *Id.*

182. Johnson, *supra* note 101 ("Those who attempt a qualified defense of using mugshots may distinguish between local media using mugshots in the context of a story, and overtly sleazy galleries… But it's important to recognize that the former very often hosts the latter… The gap between high- and low-brow mugshot tabloidism is not a great as many in the respectable media would like to believe, and a focus on the more exploitative end of the spectrum deflects responsibility from those relatively upscale outlets who do a slightly watered-down version of it"); Hutchins, *supra* note 100 (Salisbury Post editor states the paper will follow-up if suspect presents documentation that they were acquitted); Laura Hazard Owen, *Fewer Mugshots, Less Naming and Shaming: How Editors in Cleveland Are Trying to Build a More Compassionate Newsroom*, NIEMANLAB (Oct. 18, 2018), https://www.niemanlab.org/2018/10/fewer-mugshots-less-naming-and-shaming-how-editors-in-cleveland-are-trying-to-build-a-more-compassionate-newsroom/ [https://perma.cc/H8MH-3XZ5].

183. Keri Blakinger, *Newsrooms Rethink a Crime Reporting Staple: The Mugshot*, MARSHALL PROJECT (Feb. 11, 2020), https://www.themarshallproject.org/2020/02/11/newsrooms-rethink-a-crime-reporting-staple-the-mugshot [https://perma.cc/4BU4-HQ73].

184. *Id.*

185. *Id.*

186. This proposal will also likely be attacked on First Amendment grounds, as some in the legal community believe that mugshot publication itself is speech and therefore entitled to First Amendment protection. It is, however, a largely unsettled area of the law and it is not the subject of this Note.

IV. CONCLUSION

The best way forward is for Congress to limit the disclosure of mugshots until after a person has been convicted. This proposed legislation strikes the appropriate balance between privacy and the need for public disclosure. It is already a stretch to say that any public benefit is served from the distribution of mugshots; it is simply absurd to say there is one iota of necessity for the distribution of mugshots before a person is convicted unless the mugshot would help locate a fugitive. Further, mugshots have entered into the stream of interstate commerce because they are uploaded to mugshot websites, which in turn profits mugshot removal services and reputation management firms, as well as raises significant advertising revenue for local newspapers. Mugshots, therefore, are a proper subject of congressional regulation.

Another workable possibility is a modification of Section 230 to incorporate a notice system similar to the one outlined in the DMCA. This system would require search engines to remove links to websites with exploitative removal policies. No one should be able to profit off the suffering of others for simply voyeuristic purposes, particularly those who need assistance reintegrating into society.

This proposed legislation would protect millions of potentially innocent Americans from being branded "with one of the most stigmatizing and debilitating labels in our society."[187] Because of the Internet, these mugshots could haunt those who are depicted for the remainder of their lives. That is a significant price to pay for a person who has not been convicted of a crime or who has had their records sealed. Given America's love of redemption, and the public's support for criminal justice reform, the time is ripe to reconsider the existing laws surrounding mugshots.

187. *Paul*, 424 U.S. at 714 (Brennan, J., dissenting).

A Chinese Lesson in Combatting Online Counterfeits: The Need to Place Greater Obligations on Social Media as They Transform to E-Commerce Platforms

Shuyu Wang*

TABLE OF CONTENTS

* J.D., May 2021, The George Washington University Law School. B.A., Journalism, Sun Yat-sen University. Production Editor, Federal Communications Law Journal, Vol. 73. I want to thank our Adjunct Professor, Meredith Rose, for her guidance and the Federal Communications Law Journal Editors for their feedback and dedication throughout this process. I would like to also thank my family and dearest friends for their constant love and support.

I. INTRODUCTION

If you use screen time tracking apps or features on your smartphone, it is very likely that you find yourself spending most of your screen time on social media. In 2019, global users spent 50% of their mobile phone screen time on social networking and communication apps.[1] However, social media users these days gradually shift from purely "social" events to more purpose-led activities. While connecting with friends remains the main purpose for using social media, there is a usage trend towards news consumption.[2] In other words, many people use social media to "stay informed."[3]

Today, when we scroll on our news feed, we come across anything and everything—major global events like trade wars, the coronavirus pandemic, the trendiest shows on Netflix, results of an exciting NFL game, and of course, fashion trends for the next season. Social media continue to merge entertainment and commerce, creating a hub for mass consumption that allows users to research and find products to buy.[4] This is especially common among younger generations. A member of Chinese Generation Z,[5] Yifei Du, said that she uses social media to follow up with trends and get shopping tips from influencers.[6] She also sometimes generates content about her own shopping experience.[7]

Social media users' craving for shopping content revived the fashion industry after the 2008 recession.[8] Use of social media by luxury brands began to surge in 2009.[9] Social media offer great interactivity that enables luxury brands to monitor customer reviews more closely, and accordingly build the brand by increasing awareness, involvement, and engagement with customers.[10]

---

1. Sarah Perez, *App Stores Saw Record 204 Billion App Downloads in 2019, Consumer Spend of $120 Billion*, TECHCRUNCH (Jan. 15, 2020, 9:00 AM), https://techcrunch.com/2020/01/15/app-stores-saw-record-204-billion-app-downloads-in-2019-consumer-spend-of-120-billion/ [https://perma.cc/8SL3-FBBC].

2. Viktoriya Trifonova, *How Do Consumers in the West Use Social Media for Shopping?*, GLOBALWEBINDEX (May 14, 2019), https://blog.globalwebindex.com/chart-of-the-week/social-shoppers-in-the-west/ [https://perma.cc/8WZR-EG9L].

3. Olivia Valentine, *Top 10 Reasons for Using Social Media*, GLOBALWEBINDEX (Jan. 11, 2018), https://blog.globalwebindex.com/chart-of-the-day/social-media/ [https://perma.cc/U275-GB8P].

4. Trifonova, *supra* note 2.

5. Generation Z (or Gen Z for short) refers to the generation that is born around mid-to-late 1990s to the early 2010s. This is a generation that has used digital technology since a young age and is generally comfortable with the Internet and social media. *See Generation Z*, WIKIPEDIA, https://en.wikipedia.org/wiki/Generation_Z (last visited Apr. 14, 2020) [https://perma.cc/BF6E-E8YT].

6. Christine Lee, *Wise Up: The Big Mistakes Luxury Brands Are Making with China's Gen Z*, JING DAILY (May 28, 2018), https://jingdaily.com/luxury-brands-china-gen-z/ [https://perma.cc/3SAB-ZQRQ].

7. *Id.*

8. *See generally* Iris Mohr, *The Impact of Social Media on the Fashion Industry*, 15 J. APPLIED BUS. & ECON. 17 (2013).

9. *Id.* at 18.

10. *Id.*

Social media shoppers also value customer reviews more than before.[11] These consumers are wary of one-sided advertisement, and they seek human interaction to develop trust in brands before a transaction.[12] Social media, in this context, offer easy access for consumers to collect authentic reviews from other individuals. Consumers can search postings or tags for a certain brand or product to navigate among brands, informing their shopping decisions along the way.[13]

However, brands and consumers are not the only ones benefiting from the emergence of social media. Social media have become the new battlefield for combating counterfeits. Counterfeiters constantly create new accounts and postings to sell fake luxuries at almost zero cost, which makes taking down online counterfeits merchandise a "whack-a-mole" game.[14] Brand owners have to commit their limited time and resources to monitor their trademarks and continuously seek takedowns of the counterfeit listings.[15]

China, as the world's most populated country and one of the most rapidly growing economic bodies, offers global luxury brands a major e-commerce market. The constant growth in the number of Chinese social media users also sparks new opportunities for global luxury brands to penetrate the market. However, the Chinese social media ecosystem presents a great difference from the one in the Western world and unique challenges to brands. While global brands navigate the distinctive Chinese social media ecosystem, recent legal reforms in China emphasize the importance of regulating e-commerce, including establishing cyber courts and issuing the 2019 E-Commerce Law.[16] This Note will explore whether such reforms provide adequate guidance for global luxury brands to effectively enforce their trademark rights in China.

Part II of this Note will lay a foundation for discussing the common opportunities and challenges brought by social media to luxury brands. Part III will demonstrate the unique challenges brought by Chinese social media that place a greater burden on brands to monitor the market and enforce their rights. Part IV will analyze how the traditional enforcement methods in China are outdated by technological development, and how China's recent legal

---

11. *Shopper Experience Index*, BAZAARVOICE 7 (2019), https://www.bazaarvoice.com/wp-content/themes/bazaarvoice/_sei-2019/static/downloads/BV19-SEI-Main-UK-Final.pdf [https://perma.cc/BNY8-WCPK].

12. *Id.* at 16.

13. *See id.* at 10.

14. James Ray, *Trademark Enforcement: A More Nuanced Game Than Whack-a-Mole*, IPWATCHDOG (Oct. 23, 2018), https://www.ipwatchdog.com/2018/10/23/trademark-enforcement-whack-a-mole/id=102344/ [https://perma.cc/8UPM-VXHX].

15. Frederick Mostert, *Study on Approaches to Online Trademark Infringement*, WORLD INTELL. PROP. ORG. 7 (Sept. 1, 2017), https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_12/wipo_ace_12_9_rev_2.pdf [https://perma.cc/4EG4-XAU9].

16. *See, e.g.*, Sara Xia, *China's New E-Commerce Law and Its Foreign Company Impacts*, CHINA L. BLOG (Apr. 11, 2019), https://www.chinalawblog.com/2019/04/chinas-new-e-commerce-law-and-its-foreign-company-impacts.html [https://perma.cc/7YMY-RV7L]; Dani Deahl, *China Launches Cyber-Court to Handle Internet-Related Disputes*, VERGE (Aug. 18, 2017) https://www.theverge.com/tech/2017/8/18/16167836/china-cyber-court-hangzhou-internet-disputes [https://perma.cc/K4H9-NB7G].

reforms fall short on online trademark enforcement. Finally, Parts V and VI will suggest an amendment to China's E-Commerce Law that includes social media platforms as e-commerce platform operators, with a hope to place a heavier burden on Chinese social media to assist in trademark enforcement. These sections will also suggest that China's experience may better prepare brands for their enforcement on other social media in light of the U.S.' recent efforts to strengthen e-commerce regulation.

II. SOCIAL MEDIA BRING OPPORTUNITIES FOR BRANDING, ACCOMPANIED BY CHALLENGES TO ONLINE TRADEMARK ENFORCEMENT.

The emergence of social media allows luxury brands to better facilitate the word-of-mouth marketing approach.[17] Today, interpersonal communication about products and services is one of the most influential sources of marketplace information for consumers.[18] A 2018 report highlighted that 40% of luxury purchases are influenced by what consumers see online, which emphasizes the impact of social media and online channels on a luxury brand's visibility and reputation.[19]

On the other hand, social media provide a powerful tool for luxury brands to survey the market for customer behaviors and trends. The latest fashion events, product launches, or celebrity appearances might spark customer discussions on social media.[20] Hashtags on social media also help luxury brands navigate and filter customer reviews or preferences. Accordingly, brands often use social media to monitor brand reputation via online influencers in order to attract customers that align with certain social values of the brands.[21]

However, counterfeiters also benefit from the convenience of social media. Social media provide not only easy access, but also an anonymity shield that allows counterfeiters to evade identification. Even when its postings are removed or its account gets blocked, a counterfeiter can easily set up a new account in little time at no cost to continue selling fake products.[22] Furthermore, the sheer volume of counterfeit postings makes timely online monitoring and tracking extremely difficult. For example, it is estimated that Instagram might have as many as 95 million bot accounts posing as real accounts.[23] Many of these bot accounts upload an enormous

17. Mohr, *supra* note 8, at 18.

18. *Id.*

19. Sophia Guan, *93% of Consumer Engagement with Luxury Brands Happens on Instagram*, DIGIMIND (Nov. 30, 2018), https://www.digimind.com/en/news/93-of-consumer-engagement-with-luxury-brands-happens-on-instagram [https://perma.cc/LL2C-W3JT].

20. *Id.*

21. *Id.*

22. Mostert, *supra* note 15, at 3.

23. Andrea Stroppa, et al., *Instagram and Counterfeiting in 2019: New Features, Old Problems*, GHOSTDATA 6 (Apr. 9, 2019), https://ghostdata.io/report/Instagram_Counterfeiting_GD.pdf [https://perma.cc/U9D8-Q5GR].

amount of counterfeit postings every day, leading to chaotic user experiences.[24] These challenges make online trademark enforcement an unwinnable "whack-a-mole" game, where enforcers have limited whacking resources for unlimited moles.[25]

Brands are exploring ways to identify counterfeiters. Typically, the identities of online counterfeiters are only known by the platform.[26] Yet given user privacy concerns, social media platforms are reluctant to reveal identifying information to law enforcement without a subpoena.[27] Most platforms implement a notice-and-takedown system that allows intellectual property right owners to report infringing conduct to the platforms. Take Facebook as an example. Currently, under Facebook's trademark infringement reporting policy, only a trademark owner can report infringing content to Facebook, and in response, Facebook will take down infringing content and inform the fraudulent poster about the report.[28] The policy does not mention surrendering any poster's information to the trademark owner, and thus fails to provide a mechanism for brands to identify counterfeiters.[29] As a result, brands cannot completely enjoin the counterfeiters from further unlawful activities, so instead they endlessly "whack the moles" by sending infringement reports to infinity and beyond.

Civil litigation is another available yet imperfect approach. Because many of the most popular social media—including Facebook, Instagram, and Snapchat—are owned and operated by U.S. companies, brands may turn to the U.S. courts for help. Some federal circuits allow a plaintiff to use a fictitious name designation against an unidentified defendant when filing a complaint and then to amend the complaint after revealing the defendant's identity through discovery.[30] Some state court rules also allow such fictitious name designations.[31] In practice, trademark owners often subpoena social media platforms as third-party intermediaries with whom infringers engage.[32] However, even when involved in litigation, social media platforms may enforce their policies by prioritizing user information privacy over trademark owners' needs to enforce their rights. For instance, in *Nine West Dev. Corp. v. Does 1-10*, Nine West, a popular apparel brand, reported twice to Facebook

24. *Id.*

25. Mostert, *supra* note 15, at 3.

26. Maia Woodhouse, *IP Enforcement in the Digital Age: Identifying Infringers in an Anonymous Online Environment*, IPWATCHDOG (Mar. 23, 2019), https://www.ipwatchdog.com/2019/03/23/ip-enforcement-in-the-digital-age-identifying-infringers-online/id=107610/ [https://perma.cc/HE48-59FS].

27. *Id.*

28. *Reporting Trademark Infringement*, FACEBOOK, https://www.facebook.com/help/440684869305015/ (last visited Nov. 30, 2020) [https://perma.cc/B423-3L5B].

29. *See id.*

30. Edward F. Sherman, *Amending Complaints to Sue Previously Misnamed or Unidentified Defendants After the Statute of Limitations Has Run: Questions Remaining from the Krupski Decision*, 15 NEV. L.J. 1329, 1345 (2015).

31. *Id.*

32. Woodhouse, *supra* note 26.

about "fake postings" that falsely indicated Nine West as the source.[33] Facebook took down the postings and further notified the fraudulent account owner at Nine West's request.[34] Yet, Facebook refused to provide information regarding the identity of the creator of the fraudulent account.[35] In short, U.S. social media platforms rarely risk sacrificing their users' privacy at any third-party requests.

The difficulty of identifying anonymous infringers is common across the Pacific. In China, the current legal framework does not require online platform operators to disclose identifying information of infringers to trademark owners.[36] Some e-commerce platforms, such as Taobao, implement their own rules to implead third-party sellers to avoid liability when sued by trademark owners, and Chinese courts tend to recognize such an approach and do not question its legality.[37] In light of this practice, platforms, not judges, have the discretion to disclose infringers' identifying information, which may undermine the efficiency of trademark enforcement against the platforms. Nevertheless, how this approach expands to social media platforms remains to be examined through future judicial practice. Although China and the U.S. seem to have different priorities in balancing privacy rights and trademark rights, neither country's approach eases brands' burden to chase after anonymous online infringers.

III. THE UNIQUE ECOSYSTEM OF CHINESE SOCIAL MEDIA BRINGS A DIFFERENT SET OF CHALLENGES FOR LUXURY BRANDS TO ENFORCE THEIR TRADEMARKS.

Other than the common obstacles for online trademark enforcement across the world, brands also need to keep an eye on the specific challenges brought by the markets in different countries. Today, luxury brands conduct their business in the form of multinational companies (MNCs).[38] These

33. *See* Compl. at 10–14, ¶¶ 26–35, Nine West Dev. Corp. v. Does 1-10, No. 07-cv7533 (S.D.N.Y. Aug. 24, 2007), https://www.courtlistener.com/recap/gov.uscourts.nysd.312057.1.0.pdf [https://perma.cc/Y4XA-TAAB]. After bringing this suit, Nine West managed to obtain the identity of the defendants upon discovery. The court granted permanent injunction against such defendants. *See generally* Permanent Inj. and J. on Consent, Nine West Dev. Corp. v. Armon Invento and Does 1-10, No. 07-cv7533 (S.D.N.Y. Mar. 11, 2008).

34. Compl., *supra* note 33, at 11, ¶ 30; Permanent Inj., *supra* note 33 at 14, ¶ 37.

35. Permanent Inj., *supra* note 33 at 14, ¶ 36.

36. Yong Wan, et al., *Privacy Protection in China*, U. WASH. INTERMEDIARY LIABILITY RES. PROJECT 51 n.116, https://www.law.uw.edu/media/1404/china-intermediary-liability-of-isps-privacy.pdf [https://perma.cc/T4YE-9DUH].

37. *Id.* at 51–52 (providing that Taobao performs as a private judge to evaluate the trademark owner's documents regarding a suspected infringing conduct, and then discloses the infringer's identity to the court if it finds necessary).

38. Daniel C.K. Chow, *Trademark Enforcement in Developing Countries: Counterfeiting as an Externality Imposed by Multinational Companies*, *in* TRADEMARK PROTECTION AND TERRITORIALITY CHALLENGES IN A GLOBAL ECONOMY 283, 283 (Irene Calboli & Edward Lee ed., 2014).

MNCs spend great efforts on developing their brands.[39] However, brand visibility does not only matter on U.S.-based platforms like Instagram, Facebook, or Snapchat. As the MNCs move forward to develop international marketing strategies, they must keep in mind which social media are the most popular platforms in each country and how the consumers in each country engage in online shopping under the influence of social media. Enormous population and growing purchasing capability make China a desirable market for global luxury brands. According to a Statista report, the number of social network users worldwide amounted to 3.4 billion in 2019.[40] Disaggregating this number, China possessed 882.23 million users and ranked first among all countries,[41] while the United States ranked third with 219.86 million users.[42]

With a combination of huge user numbers and platform variety, Chinese social media provide a significant opportunity for luxury brands to solicit large-quantity sales. For example, Burberry was recognized as the first luxury brand to use social media for flash sale marketing in China.[43] On August 17, 2018, China's Valentine's Day, Burberry launched a mini-program[44] on WeChat, the most popular social media platform in China, to sell two new handbags exclusive to the Chinese market.[45] Later that year, Christian Dior became the first luxury brand to leverage livestream to sell its beauty products on WeChat.[46] This hour-long livestream took place on November 16, 2018, and attracted more than three million visitors.[47]

However, Chinese social media possess some significantly distinctive features, creating additional difficulty for global luxury brands to navigate. This sharp distinction stems from the implementation of the Great Firewall of China. Due to China's strict government control over Internet content, the global social media giants—Facebook, Twitter, and Instagram—are

39. *Id.* at 284.

40. *Social Networks in China*, STATISTA 2 (Nov. 7, 2019), https://www-statista-com.proxygw.wrlc.org/topics/1170/social-networks-in-china/#dossierSummary__chapter1.

41. *Id.* at 3, 8.

42. *Number of Social Network Users in the United States from 2017 to 2025*, STATISTA (July 15, 2020), https://www.statista.com/statistics/278409/number-of-social-network-users-in-the-united-states/ [https://perma.cc/WH3P-8WBC].

43. Tasmin Smith, *Exclusive: Burberry Launches 2 Handbags Just for China on First WeChat Mini-Program*, JING DAILY (Aug. 3, 2018), https://jingdaily.com/burberry-wechat-mini-program/ [https://perma.cc/R8YY-VCBH].

44. "Mini-programs" are lightweight apps that run inside another app, such as WeChat. They don't need to be downloaded or upgraded through app stores. They make it possible for one app to perform the service of many apps combined. Julianna Wu, *Mini Programs: The Apps inside Apps that Make WeChat So Powerful*, S. CHINA MORNING POST (Feb. 27, 2019, 6:11 AM), https://www.abacusnews.com/who-what/mini-programs-apps-inside-apps-make-wechat-so-powerful/article/3000920 [https://perma.cc/UR2M-LU5R]; *see also infra* Part III. A.

45. Smith, *supra* note 43.

46. Yiling Pan, *In an Industry First, Dior Beauty Debuts Livestreaming Sales on WeChat*, JING DAILY (Nov. 16, 2018), https://jingdaily.com/dior-livestreaming-wechat/ [https://perma.cc/M6QW-FLMP].

47. *Id.*

inaccessible in China.[48] In response, China's Internet companies gradually developed a different set of social media platforms that better adapt to Chinese users' needs and preferences.[49] As a result, brands may find their enforcement strategies on Facebook or Instagram non-applicable to the Chinese market. Thus, luxury brands are driven by the need to exploit the Chinese market to explore the unique features of Chinese social media.

A. The "All-In-One" Feature of China's Major Social Media Encourages Embedding In-App Checkout Methods, Which Creates a Closed-Up Environment for Social Shopping.

Many social media in China were created first as messaging or blog-posting platforms. However, many have evolved into an "all-in-one" hybrid, enabling users to accomplish all kinds of tasks within one platform.[50] Among all services provided on such hybrid platforms, the implementation of a quick and easy in-app checkout feature is most relevant here.

An in-app checkout feature allows users to make a purchase without leaving the social media app and provides a smoother experience of social shopping.[51] In China, WeChat serves as the most important portal to channel users for brands. Since 2017, WeChat has been experimenting a new model of e-commerce—it started to integrate "mini-programs," which are embedded inside the main WeChat app as sub-ports for merchants to further interact with their followers and potential customers.[52] For brand owners seeking a more efficient and direct way to connect to buyers, mini-programs provide merchants with new ways to sell products.[53] Mini-programs grant freedom for brands to independently design their shop page interface and also access and analyze customer data as they please, which lowers customer acquisition costs for brands.[54] Also, along with other features embedded inside WeChat, such

---

48. *How Is Social Media Different in China from The West?*, MOBVISTA (May 23, 2019), https://www.mobvista.com/en/blog/social-media-different-china-west/ [https://perma.cc/4A78-K6LW].

49. *See Social Media and Censorship in China: How Is It Different to the West?*, BBC NEWS (Sept. 26, 2017), http://www.bbc.co.uk/newsbeat/article/41398423/social-media-and-censorship-in-china-how-is-it-different-to-the-west [https://perma.cc/PM94-ARUS].

50. *See, e.g.*, Yuan Ren, *Know Your Chinese Social Media*, N.Y. TIMES (Nov. 19, 2018), https://www.nytimes.com/2018/11/19/fashion/china-social-media-weibo-wechat.html [https://perma.cc/N9E6-JUD3].

51. *See* Daniel Keyes, *Instagram Is Moving Toward Becoming a Full-Blown E-commerce Platform*, BUS. INSIDER (May 2, 2019), https://www.businessinsider.com/instagram-in-app-checkout-feature-2019-5 [https://perma.cc/B6DG-XRT8].

52. Mini programs are not exclusively designed for users who may act as online merchants. In fact, mini programs are available to general WeChat users and they provide more functions than marketplace.

53. Eva Xiao, *In WeChat, Sellers Are Experimenting with New Models of Ecommerce*, TECH IN ASIA (Jan. 19, 2018), https://www.techinasia.com/wechat-mini-programs-ecommerce [https://perma.cc/KZL7-GU3A].

54. *See* Franklin Chu, *Why China Ecommerce Is Going Crazy for WeChat Mini-Programs*, DIGIT. COMM. 360 (Apr. 16, 2019), https://www.digitalcommerce360.com/2019/04/16/why-china-ecommerce-is-going-crazy-for-wechat-mini%E2%80%91programs/ [https://perma.cc/RSJ4-ZHGE].

as mobile wallet and group-chat sharing, mini-programs allow merchants to direct users from their subscription posts to the shop page and encourage users to share the link with friends to obtain group-shopping coupons, all of which can be done with a few taps, without leaving the one app.[55]

More importantly, WeChat presents almost zero limitations for entities to open stores via mini-programs as long as required qualification documents are provided for verification.[56] This boosts e-commerce in China farther. In 2018, the number of mini-programs reached 1 million, which was half the size of the Apple App Store that year.[57] The next year, Tencent, the company that owns WeChat, announced that its users spent 800 billion Chinese yuan ($115 billion USD) through mini-programs in 2019.[58] The company also intended to focus more on adding merchants and services to mini-programs in 2020, which seems to signal that Tencent is increasing its competitiveness in the e-commerce field.[59]

On the other hand, dominant social media in other parts of the world are also exploring ways to integrate shopping features inside the platforms, but their approaches generally contrast with WeChat's openness to business entities. In 2018, Instagram allowed "shoppable posts," a feature that showed the price tag of the displayed products and a direct link to the shopping website.[60] This feature was somewhat cumbersome, because the users were re-directed to external links and had to experience the annoying checkout process every time they placed an order.[61] One year later, Instagram enabled in-app checkout for those shoppable posts.[62] The new feature allows users to purchase items with stored payment information without leaving the app, but it comes at the price of merchants paying a "seller's fee" to enable the

55. Xiao, *supra* note 53.

56. *See generally Service Categories Available for Mini Programs*, WECHAT OFF. DOCUMENTS (微信官方文档), https://developers.weixin.qq.com/miniprogram/en/product/material/#Service-Categories-Available-for-Mini-Programs-Owned-by-Entities-Other-Than-Individuals (last visited Apr. 11, 2020) [https://perma.cc/4PN8-AYGF]. This page lists the required qualifications documents for non-individuals, individuals and overseas entities to apply for mini program operation. These documents are in general mandated by the Chinese government for regulating commerce, but not for WeChat's own purpose to review the qualifications of business operators.

57. Rita Liao, *WeChat Reaches 1M Mini Programs, Half the Size of Apple's App Store*, TECHCRUNCH (Nov. 7, 2018), https://techcrunch.com/2018/11/07/wechat-mini-apps-200-million-users/ [https://perma.cc/6JYJ-XGG5].

58. Masha Borak, *WeChat Mini Programs Are Becoming a Lot More Important for Tencent*, S. CHINA MORNING POST: ABACUS (Jan. 9, 2020 8:39 PM), https://www.scmp.com/abacus/tech/article/3045430/wechat-mini-programs-are-becoming-lot-more-important-tencent [https://perma.cc/4REY-JJZV].

59. *Id.*

60. Arielle Pardes, *Instagram's New Shopping Feature Makes It a Digital Mall*, WIRED (Mar. 19, 2019, 8:00 AM), https://www.wired.com/story/instagram-in-app-shopping-feature/ [https://perma.cc/TK8K-HKFJ].

61. *Id.*

62. Josh Constine, *Instagram Launches Shopping Checkout, Charging Sellers a Fee*, TECHCRUNCH (Mar. 19, 2019, 9:33 AM), https://techcrunch.com/2019/03/19/instagram-checkout/ [https://perma.cc/8BU9-74L8].

"Checkout with Instagram" option, and is only available to selective partner brands.[63]

In March 2019, Facebook also expressed an interest in social shopping by shifting its focus to building a one-stop shop messaging service that combines everything the company has to offer.[64] Although there are many differences between Facebook and WeChat, the "everything-app" ambition of the two companies seems to point in the same direction, which is to implement as many essential functions as possible to encourage users to stay within one app.[65]

Meanwhile, Snapchat seeks to mine its way to social shopping by making use of online influencers, but only selective ones. In June 2019, Snapchat launched in-app stores for five of its most powerful influencers, namely Kylie Jenner (Kylie Cosmetics), Kim Kardashian (KKW Beauty), Shay Mitchell (Béis), Spencer Pratt (Pratt Daddy Crystals), and Bhad Bhabie (BHADgoods).[66] Snapchat users can now purchase directly from these brands with the swipe-up feature that is built inside the app.[67]

Although U.S. platforms have started integrating in-app checkout features, the total revenue generated in this way contributes to a relatively small portion of online sales.[68] In 2018, social media commerce drew $16.94 billion in the U.S., which was only 3% of the $513.61 billion in online sales estimated by the U.S. Department of Commerce for the year.[69] In contrast, social media commerce in China counts for more of online shopping, comprising 8.5% of online sales in 2017.[70] Analysts project social media commerce to increase into 2022, reaching 15% of e-commerce, or $413 billion in sales.[71]

That said, there are some underlying IP concerns despite the robust e-commerce growth on Chinese social media platforms. First of all, WeChat, like other social media, does not function as a search engine. The lack of organic search makes it harder for brands to monitor their trademark in the closed-up platform.[72] Second, the in-app checkout feature replaces the

---

63. *Id.*

64. Nick Statt & Shannon Liao, *Facebook Wants to Be WeChat*, VERGE (Mar. 8, 2019, 1:12 PM), https://www.theverge.com/2019/3/8/18256226/facebook-wechat-messaging-zuckerberg-strategy [https://perma.cc/8ZNY-NQMU].

65. *Id.*

66. Kerry Flynn, *Ahead of "Shop" Button for Publishers, Snapchat Launches In-App Stores for Snap Influencers*, DIGIDAY (June 6, 2019), https://digiday.com/marketing/snapchat-stores-influencers-shop/ [https://perma.cc/VZK9-D7SH].

67. *Id.*

68. Daniela Wei & Shelly Banjo, *The Future of Shopping Is Already Happening in China*, BLOOMBERG (Apr. 24, 2019, 4:00 PM), https://www.bloomberg.com/news/articles/2019-04-24/china-s-gen-z-skips-the-stores-and-shops-on-social-media [https://perma.cc/GN4L-DLUN].

69. *Id.*

70. *Id.*

71. *China's Retail Sales Are Growing Fast on Social Media*, MARKETPLACE (May 7, 2019), https://www.marketplace.org/shows/marketplace-tech/china-livestreaming-boosting-retail/ [https://perma.cc/FY6K-QEAR].

72. *See What is a WeChat Shop?*, WALKTHECHAT, https://walkthechat.com/wechat-shops/ (last visited on Apr. 12, 2019) [https://perma.cc/2JKR-NSGF].

inbound links to merchants' websites outside the app, with which brands may track the domain name to the registration information and find out who the infringers are. Last but not least, the low threshold of registering a mini-program shop challenges WeChat's ability to screen the merchants.[73] Within only one year of the open test of mini-programs, WeChat shut down 875 mini-programs for selling fake goods.[74] It is unclear whether Tencent can effectively manage shops on WeChat mini-programs to address IP infringement issues like counterfeit goods.[75]

B. The Social Media Landscape in China Is More Fragmented, Requiring Brands to Exert Greater Efforts to Monitor the Whole Market.

While WeChat remains the most popular "everything app" in China, there are other apps in the Chinese social media ecosystem that satisfy different user needs, making the social media landscape quite fragmented. One possible reason for fragmentation is that the domestic market in China is so big that platforms can fragment their appeal to demographic slices or geographic areas without competing against each other.[76] More and more social media are capitalizing on marketing to users' shopping needs. By implementing third-party in-app payment methods, these social media potentially enable counterfeiters to dilute the platform as a sales channel.[77]

When it comes to shopping review app, perhaps the most popular one in China is "Xiaohongshu" (which is literally translated as "Little Red Book"). Created in 2013 as an online community to share product reviews and lifestyle posts, Xiaohongshu attracts millions of users who want to learn about others' shopping experiences before they make their own decision to purchase.[78] Also, users typically visit Xiaohongshu to see what is trendy. Thus, Xiaohongshu is a platform that thrives on user-generated content ("UGC"), and users can add "product tags" to their postings that further direct readers to a brand's page.

In response to users' strong desire to follow the trend by purchasing the products promoted by influencers, Xiaohongshu gradually expanded from a shopping directory to a hybrid social media and e-commerce platform.[79] It

---

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

74. Weixin Pai (微信派), *Guanyu Daji "Jiahuo, Gaofang" Lei Xiaochengxu de Gonggao* (关于打击"假货、高仿"类小程序的公告) [*Announcement on Cracking Down on "Fake and High Imitation" Mini-Programs*] (Jan. 23, 2018), https://mp.weixin.qq.com/s/I03kuKi9liQWLJwwsRYrPw [https://perma.cc/VQL6-YRNZ].

75. Xiao, *supra* note 53.

76. *How is Social Media Different in China from The West?*, *supra* note 48.

77. *See Counterfeits on TikTok: IP Enforcement Best Practices*, WORLD TRADEMARK REV. (June 10, 2019), https://www.worldtrademarkreview.com/brand-management/counterfeits-tiktok-ip-enforcement-best-practices [https://perma.cc/28ZA-P7U7].

78. Chencen, *Xiaohongshu Is Becoming a Giant in Both Social Media and E-Commerce*, DAXUE CONSULTING (Mar. 22, 2019), https://daxueconsulting.com/latest-facts-and-insights-about-xiaohongshu-2019/ [https://perma.cc/VL74-BW4B].

79. *See generally id.* (discussing the development of Xiaohongshu).

now embeds an in-app marketplace, the RED Mall, where users can search and purchase goods directly within the app.[80] It also provides "product suggestions" as shopping entries under a brand's introduction page, which link to the UGC tagged with the brand's name.[81] Unsurprisingly, many brands leverage the platform to improve visibility and interaction with potential customers,[82] and around 20,000 brands have set up official accounts on the platform, including some very well-known brands like Tom Ford Beauty, Tiffany & Co., and Guerlain.[83]

However, the products supplied on the RED Mall face a credibility challenge. Some products are listed as "sold by verified merchants," which creates an impression that users are purchasing from official stores. However, some users have complained that they bought counterfeits from "official stores" on the platform.[84] Apart from cheap knockoffs sold as "verified official products," there are about 10,000 third-party sellers on the RED Mall, creating an additional set of problems for legitimate brands to monitor their trademarks.[85]

Another example is Douyin/TikTok. Started as a short video platform where users share their life moments and creativity through 15-second clips, TikTok has swept both the Chinese and Western markets. Witnessing TikTok's great success, loads of brands launched their content campaigns on this platform.[86] In April 2019, Hollister tested TikTok ads that included "shop now" buttons, which would bring users to shopping sites inside the app.[87] Other retailers, like Poshmark, have also advertised on the app.[88]

While Western advertisers have dabbled with TikTok—without engaging its e-commerce functions—the Chinese version of this app, Douyin, succeeded in converting its user traffic to millions of dollars with a "shop now" button.[89] In 2018, Bytedance (the developer company of Douyin and

---

80. *See* Corsearch, *The Facts about RED (Xiaohongshu 小红书): Counterfeits, RED and Brand Enforcement*, MEDIUM (Jan. 16, 2020), https://medium.com/@Corsearch/the-facts-about-red-xiaohongshu-%E5%B0%8F%E7%BA%A2%E4%B9%A6-counterfeits-red-and-brand-enforcement-pointer-brand-b912866e081 [https://perma.cc/HP5F-7GPQ].

81. *See generally Little Red Book: From User Experience to Strategy, Leverage Xiaohongshu Now!*, DIGIT. BUS. LAB (Jan. 28, 2019), https://digital-business-lab.com/2019/01/leverage-little-red-book/ [https://perma.cc/FCQ2-PE5R].

82. *See id.*

83. *See* Corsearch, *supra* note 80.

84. *See generally Jiahuo Tousu Fanlan, Shenxian Xinren Weiji de Xiaohongshu Nengfou Poju?* (假货投诉泛滥 深陷信任危机的小红书能否破局？) [*With Complaints about Fake Goods Abound, Can Xiaohongshu Break Free from the Trust Crisis?*], SINA.COM (Apr. 29, 2019, 06:57 AM), https://tech.sina.com.cn/i/2019-04-29/doc-ihvhiqax5630134.shtml [https://perma.cc/ZV43-5VJB].

85. *See* Corsearch, *supra* note 80.

86. Cale Guthrie Weissman, *How Tiktok Is Testing In-app E-Commerce*, DIGIDAY (July 10, 2019), https://digiday.com/retail/tiktok-testing-app-e-commerce/ [https://perma.cc/8BF8-PELS].

87. *Id.*

88. *Id.*

89. James Hale, *TikTok Is a Mostly Untapped Space for Western Ecommerce — But Chinese Companies are Using it to Make Millions*, TUBEFILTER (July 10, 2019), https://www.tubefilter.com/2019/07/10/tiktok-douyin-ecommerce-marketing-does-tiktok-monetize/ [https://perma.cc/7YJH-LTEM].

TikTok), partnered with e-commerce company Alibaba, which owns Taobao, the largest online shopping platform in China. Together, Bytedance and Alibaba offered a "Shop Now" button embeddable in short videos to Douyin accounts with more than one million followers.[90] The button redirects viewers to Taobao via a single-click product link. This new feature brought great profits in a short amount of time. In December 2018, Bytedance said that adding the button generated considerable sales in just one day, amounting to 200 million Chinese yuan ($29 million USD).[91] Subsequently, Douyin made the function available to more users, "lowering the threshold from those with one million followers down to just eight thousand followers and more than ten posts."[92]

As a result, this content sharing platform has become another outlet to display counterfeits. A search for keywords such as "luxury" and "prestige watches" on Douyin would likely return plenty of postings of fake luxury goods.[93] Some suspected fake product videos even receive Douyin's algorithmic recommendations.[94] What's more, the core functions of Douyin—short videos and live streaming—can easily evade the traditional IP enforcement methods relying on text and image searches.[95] Hence, traditional enforcement tactics relying on automated scraping tools to collect data for review become "obsolete," resulting in greater difficulty for trademark monitoring.[96]

Other social media also target specialized markets based on a certain type of product or service. Even though they are not necessarily tied to the luxury market, they underscore that the line between social media and e-commerce platforms in China is vanishing. Bilibili, for example, exemplifies how video platforms comparable to YouTube monetize user traffic. Bilibili is one of the most popular video sharing platforms in China, themed around animation, comics, and gaming ("ACG") culture, where users can submit, view, and add commentary subtitles on videos.[97] It also integrates an in-app marketplace that sells event tickets and ACG derivative products.[98] Users can directly purchase goods within the app with embedded third-party payment methods. According to Bilibili's first-quarter report of 2019, the profits

90. *Id.*
91. *Id.*
92. *Id.*
93. Eva Yoo, *Short Video Platforms Douyin, Kuaishou Accused of Showing Counterfeit Products*, TECHNODE (Mar. 26, 2018), https://technode.com/2018/03/26/douyin-kuaishou-counterfeit-products/ [https://perma.cc/T9YW-ZLVU].
94. *Id.*
95. *Counterfeits on TikTok*, *supra* note 77.
96. *Id.*
97. Steffi Noel, *The Commercialization of the Bilibili Platform with a New E-commerce Function*, DAXUE CONSULTING (June 24, 2019), https://daxueconsulting.com/commercialization-bilibili-platform/ [https://perma.cc/WHH3-VH9R].
98. *See id.*

derived from e-commerce consisted of 7% of the total quarterly revenue of the company, amounting to 15 million dollars.[99]

Other examples of apps with in-app markets include "Netease Cloud Music," a music streaming service like Spotify with user comment features. Netease Cloud Music has a plugged-in store in its app that allows users to buy sound recording products, musical instruments, and many other music-related items.[100] Another app, "Xiachufang," an online recipe-sharing community, also has a marketplace where cooking stencils and meal kits are being sold.[101] Users reading recipes, for example, may find links directing them to purchase the materials for a dish they are interested in, of course, without leaving the app.

How much profit these actions will generate remains to be tested, but it is an obvious, growing trend that Chinese social media are trying to forge a new e-commerce approach by combining the socializing behaviors and shopping desires of users. Facing the challenges brought by this new trend, luxury brands must develop counterfeit combating tactics that are able to keep pace with technological developments.

IV. THE CURRENT LEGAL SCHEMES IN CHINA CANNOT PROMISE A POSITIVE EXPECTATION FOR TRADEMARK ENFORCEMENT

A. Traditional Trademark Enforcement Methods Cannot Adequately Adapt to the Context of Social Media.

To address the criticism of weak IP protection, China tries to improve its IP enforcement methods to stay aware of the nation's growing economy.[102] The current enforcement methods remain the same as before the rise of social media: administrative raids, civil actions, and criminal prosecutions.[103] However, social media enable new infringing behaviors that old legal

99. *See BZhan Fabu 2019nian Q1 Caibao: Zongyingshou Dadao 13.7yi Yuan, Youxi Shouru Zhanbi 64%* (B 站发布 2019 年 Q1 财报：总营收达到 13.7 亿元，游戏收入占比 64%) [*Bilibili Released Q1 Financial Results in 2019: the Total Revenue Reached 1.37 Billion Yuan, with Game Revenue Accounting for 64%*], BILIBILI.COM (May 14, 2019), https://www.bilibili.com/read/cv2686898/ [https://perma.cc/2C2C-JZ69].

100. Netease Cloud Music has a web version of its store, which is the same as the one in the mobile app but with a different interface. The web version is available here: NETEASE CLOUD MUSIC, https://music.163.com/store/product (last visited Dec. 1, 2020) [https://perma.cc/WN7M-59BZ].

101. *See* Yingzhao Zhu, *A UI/UX Design Walk-Through of Xiachufang, a Leading Chinese Recipe App*, MEDIUM (Oct. 18, 2019), https://medium.com/@yingzhaozhu/a-ui-ux-design-walk-through-of-xiachufang-a-leading-chinese-recipe-app-32bbe7fdf3db [https://perma.cc/X8DQ-8V4E].

102. Jennifer Lei, Note, *Makeup or Fakeup?: The Need to Regulate Counterfeit Cosmetics Through Improved Chinese Intellectual Property Enforcement*, 88 FORDHAM L. REV. 309, 317 (2019).

103. *See generally id.* at 317–22.

schemes failed to anticipate, and thus bring new challenges to the existing enforcement framework.

1. Raids by Administrative Agencies

The most frequently utilized enforcement method in China is administrative raids on warehouses.[104] The State Administration for Market Regulation ("SAMR") carries out this function by working with local law enforcement to raid stores, factories, and warehouses containing counterfeit products upon trademark owners' petitions.[105] SAMR has the authority to determine infringement while executing the raids and, upon an infringement finding, SAMR can opt to destroy or confiscate infringing goods, or fine the infringers.[106]

Because of the public exposure and the fast and inexpensive results, foreign companies tend to enforce their rights through raids.[107] Yet, despite the popularity, administrative raids barely deter counterfeit goods, because counterfeiters can easily return after the raids with a similar name or mark.[108] As discussed in Part II above, the rise of social media worsens the situation. The "whack-a-mole" game perpetuates because of the low cost and high efficiency of setting up new accounts on social media platforms.[109] Furthermore, the failure to identify an anonymous online counterfeiter often hinders brands' ability to seek administrative raids, because there is "no one" to enforce against.[110]

2. Civil Actions Against Counterfeiters and Trademark Infringers

Since the implementation of specialized IP courts in Beijing, Shanghai, and Guangzhou since 2014, China has witnessed a drastic increase in IP litigation.[111] However, foreign companies do not rely on litigation to enforce trademark rights because of the lengthy proceeding or the lack of preliminary injunctions.[112] Besides, damages are typically low, thereby disincentivizing litigation.[113]

Social media presents other challenges to enforcing trademark rights through civil actions. Although filing a complaint requires at least some basic information to identify the counterfeiter, there is no legal mechanism

104. *Id.* at 317.
105. *Id.* at 318.
106. *Id.*
107. Lei, *supra* note 102, at 318–19; Adela Hurtado, Note, *Protecting the Mickey Mouse Ears: Moving Beyond the Traditional Campaign-Style Enforcement of Intellectual Property Rights in China*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 421, 436–37 (2018).
108. *See* Lei, *supra* note 102, at 319.
109. *See generally supra*, Part II; *see also* Mostert, *supra* note 15, at 3, 7.
110. *See* Woodhouse, *supra* note 26.
111. Lei, *supra* note 102, at 320.
112. *Id.* at 320–21.
113. *Id.* at 321.

available to compel the social media platforms to provide identifying information.[114] Besides, the sheer volume of fake luxury product accounts on the platforms makes it impractical for brands to chase after every infringer, so the volume of counterfeit products and their potential harm to the market is unidentifiable merely from an account itself. From a management perspective, brands will seldom choose to chase after a single counterfeiter account in the face of a huge cost of litigation.

3. Criminal Prosecution

Criminal prosecution for IP enforcement is possible under China's Criminal Law, but it is practically unviable due to the scattered nature of counterfeit storages.[115] The government will often ignore small and medium scale infringing activities as insignificant, but instead prosecute infringers for large operations that violate the rights of the biggest brands.[116] In China, criminal prosecution of trademark cases consisted of less than 1.50% of all IP cases in 2018.[117]

B. China's New Cyber Courts and E-Commerce Law Improve Online Infringement Enforcement, Yet They Still Fall Short on Trademark Enforcement on Social Media.

Given the huge progress and great economic growth achieved in e-commerce, China has been experimenting with new ways to better regulate this area. In the past few years, China made several groundbreaking changes to its legal system. The most significant changes are the implementation of cyber courts and the issuance of the e-commerce law.

China established its first cyber court in 2017 in Hangzhou, known as the "capital of Chinese e-commerce," where the e-commerce tycoon Alibaba and many other Internet companies sit.[118] By creating the cyber court, China addressed the drastic increase in the number of Internet-related claims.[119] Within one year, the Hangzhou Court of the Internet accepted more than

114. *See supra* Part II.

115. Lei, *supra* note 102, at 321.

116. *Id.* at 322.

117. *2018 Xinshou Zhishi Chanquan An Chao 33wan Jian* (2018 新收知识产权案超 33 万件) [*More than 330,000 New IPR Cases Were Received in 2018*], XINHUA.NET (Apr. 23, 2019, 7:25 AM), http://www.xinhuanet.com/tech/2019-04/23/c_1124401581.htm [https://perma.cc/W2FP-7A7U].

118. Dani Deahl, *China Launches Cyber-Court to Handle Internet-Related Disputes*, VERGE (Aug. 18, 2017, 4:33 PM), https://www.theverge.com/tech/2017/8/18/16167836/china-cyber-court-hangzhou-internet-disputes [https://perma.cc/Y25K-NP8J].

119. *See id.*

12,000 Internet-related cases and concluded more than 10,000 of them.[120] Shortly after the establishment of the Hangzhou Court of the Internet, China launched two more cyber courts in Beijing and Guangzhou to further explore implementing high technology to improve judicial efficiency.

The difference between cyber courts and traditional courts mainly lies in the procedures. The cyber courts do not require physical attendance.[121] All documents, including filings, evidence submission, payment, and service of documents, are processed online.[122] The courts also adopt video conference technology to conduct hearings and mediations.[123] These changes lower costs for parties to attend judicial proceedings and thus improve the courts' efficiency.[124]

Another groundbreaker is the issuance of China's new statute governing e-commerce, the P.R.C. E-Commerce Law.[125] China passed the E-Commerce Law in August 2018 and effectuated it on January 1, 2019.[126] It hikes pressure on online retailers to tackle counterfeit products on their platforms.[127] This new law applies to three types of operators: e-commerce platform operators, third-party merchants who utilize e-commerce platforms to sell goods and services, and online vendors "operating their own websites or doing business via other network channels, such as social media sites."[128] This last category indicates that the law extends to merchants who sell goods through WeChat or Douyin/TikTok.[129] The law also addresses the compliance requirements for platform operators and merchants, such as identity

120. *Zuigao Renmin Fayuan: Gongzheng & Xiaolü, Zai Wangluo Hulian Hutong—Xiezai Hangzhou Hulianwang Fayuan Guapai Chengli Yizhounian Zhiji* (最高人民法院：公正&效率，在网络互联互通——写在杭州互联网法院挂牌成立一周年之际) [*Supreme People's Court: Justice and Efficiency Intersecting on the Internet—A Message for the First Year Anniversary of the Inauguration of the Hangzhou Court of the Internet*], SUP. PEOPLE'S CT. (Aug. 20, 2018, 08:53 AM), http://www.court.gov.cn/zixun-xiangqing-112931.html [https://perma.cc/4JD7-77KE].

121. Paolo Beconcini, *More "NetCourts" Opening in China*, SQUIRE PATTON BOGGS (Nov. 14, 2018), https://www.iptechblog.com/2018/11/more-netcourts-opening-in-china/ [https://perma.cc/6UWH-ANB2].

122. *Id.*

123. *Id.*

124. *China Opens Its First "Cyber Court"*, YAHOO.COM (Aug. 18, 2017), https://www.yahoo.com/entertainment/china-opens-first-cyber-court-110619464.html [https://perma.cc/GAH6-TM2H].

125. Zhonghua Renmin Gongheguo Dianzi Shangwu Fa (中华人民共和国电子商务法) [P.R.C. E-Commerce Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug, 31, 2018, effective Jan. 1, 2019), *translated in* CHINA LAW TRANSLATE.COM (https://www.chinalawtranslate.com/en/p-r-c-e-commerce-law-2018/ [https://perma.cc/52ZA-HUGB]) [hereinafter E-Commerce Law].

126. Zen Soo, *Here's How China's New E-Commerce Law Will Affect Consumers, Platform Operators*, SCMP (Jan. 1, 2019, 6:02 AM), https://www.scmp.com/tech/apps-social/article/2180194/heres-how-chinas-new-e-commerce-law-will-affect-consumers-platform [https://perma.cc/9YQN-2RC8].

127. *Id.*

128. *Id.*

129. *Id.*

verification, recordkeeping, tax conformance, and intellectual property protection.[130]

It seems likely that the establishment of the cyber courts and the passage of the E-Commerce Law would allow global brands to bring trademark infringement or unfair competition claims more easily against Chinese counterfeiters. But in practice, several limitations hinder the quick and effective enforcement that global brands seek.

1. Issue One: Jurisdiction of Cyber Courts

The Internet allows a huge number of parties at different locations to enter into one business affair at the same time. If any dispute arises, it is impractical to track every anonymous party in the cyberworld to its real identity in the physical world. The establishment of the cyber courts aims to bypass the difficulty of locating the defendant in Internet-related cases, but still, it does not help much for identifying an anonymous infringer.

Traditionally in China, a plaintiff must provide the defendant's residential information to satisfy territorial jurisdiction to file a suit in a certain court.[131] Otherwise, a plaintiff must prove that the dispute relates to a particular territory to show subject-matter jurisdiction.[132] The Internet places an extra burden on both issues. Defendants often reside in jurisdictions from the jurisdictions of online platforms, and it takes great effort to locate a specific Internet service user even with IP address trackers.[133] And since the Internet is borderless, it is difficult to pin a "place" where a dispute arises.[134] The Supreme People's Court of China ("SPC") explained that the "location" of a tort on an information network includes where the computer and other pieces of information equipment used to commit the alleged tort are located.[135] Consequently, the omnipresence of Internet service infrastructure creates multiple connections between a tort and a variety of jurisdictions,

130. *See generally* E-Commerce Law, *supra* note 125.

131. *See* Lin Yifu, *Rethinking the Territorial Jurisdiction of the Chinese Internet Courts*, STL L. REV. BLOG (Apr. 17, 2019), https://stllawreview.com/index.php/2019/04/17/rethinking-the-territorial-jurisdiction-of-the-chinese-internet-courts/ [https://perma.cc/7Z9C-MK6M].

132. *See id.*

133. Xiao Jianguo (肖建国) & Zhuang Shiyue (庄诗岳), *Lun Hulianwang Fayuan Shewang Anjian Diyu Guanxia Guize de Goujian* (论互联网法院涉网案件地域管辖规则的构建) [*Rule Construction on the Territorial Jurisdiction of the Cyber Courts*], 3 J. L. APPLICATION 16, 17 (2018).

134. *Id.* at 16–17.

135. Zuigao Renmin Fayuan Guanyu Shiyong Zhonghua Renmin Gongheguo Minshi Susong Fa de Jieshi (最高人民法院关于适用《中华人民共和国民事诉讼法》的解释) [Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China] (Jan. 30, 2015), art. 25, *translated in* IPKEY (https://ipkey.eu/sites/default/files/legacy-ipkey-docs/interpretations-of-the-spc-on-applicability-of-the-civil-procedure-law-of-the-prc-2.pdf [https://perma.cc/DTQ9-W9YN]). SPC's judicial interpretation is a source of law in China that has less authority weight than statute. But in practice, many lawyers rely on SPC's judicial interpretation for detailed explanation of vague statutory language.

enabling defendants to transfer their cases to jurisdictions that serve their best interests.

In contrast, the cyber courts lessen the burden of proving territorial jurisdiction over a defendant. The cyber courts have cross-regional jurisdiction over all Internet-related cases that fall within the subject-matter jurisdiction categories.[136] As long as a plaintiff (namely any foreign brand owner in this context) can show a "genuine connection" with respect to Hangzhou, Beijing, and Guangzhou, the cyber courts obtain territorial jurisdiction.[137] Arguably, a plaintiff can easily prove a connection because a majority of Internet companies with thriving business are headquartered or have their principal place of business in these three cities.[138] Therefore, foreign brand owners no longer need to pin down an ultimate territory to bring a valid claim. Rather, they may satisfy the territorial jurisdiction requirement simply by connecting any disputes to the social media platform's principal place of business.

However, foreign brand owners may nevertheless suffer from the limitations posed by subject-matter jurisdiction of the cyber courts. Currently, the cyber courts only have jurisdiction over an exclusive list of issues:

- Disputes regarding online purchases of goods, online service agreements, and small-amount loan agreements that will be further performed via online services;
- Disputes regarding "Internet copyright" ownership and infringement;
- Infringement on personal rights (*e.g.* defamation) using the Internet;
- Product liability claims for goods purchased online;
- Domain name disputes;
- Disputes arising from Internet-based administration; and
- Other civil and administrative cases concerning the Internet assigned to the Cyber-court by a higher court.[139]

A plain reading of the subject-matter jurisdiction categories of the cyber courts does not favor foreign brands owners' position. The dispute between

136. Xiao & Zhang, *supra* note 133, at 18; *see infra* note 139 for the "subject-matter jurisdiction categories."

137. *Id.* at 21.

138. Lai Lin Thomala, *Distribution of Unicorn Companies from Internet and Information Technology (IT) Industry in China as of December 2019, by Region*, STATISTA (Aug. 27, 2020), https://www.statista.com/statistics/1129137/china-share-of-unicorn-internet-and-information-technology-companies-by-region/ [https://perma.cc/9HLX-X3UX].

139. Sara Xia, *China Establishes Its First Cyber-Court in Hangzhou: Thank You Alibaba*, HARRIS BRICKEN (Aug. 16, 2017), https://www.chinalawblog.com/2017/08/china-establishes-its-first-cyber-court-in-hangzhou-thank-you-alibaba.html [https://perma.cc/9PJN-PXY2]. The cited list above is condensed from the eleven categories provided by the Supreme People's Court's announcement. *See* Zuigao Renmin Fayuan Guanyu Hulianwang Fayuan Shenli Anjian Ruogan Wenti de Guiding (最高人民法院关于互联网法院审理案件若干问题的规定) [Provisions of the Supreme People's Court on Several Issues Concerning the Hearing of Cases by Internet Courts] (promulgated by Sup. People's Ct., Sep. 6, 2018, effective Sep. 7, 2018).

brands and counterfeiters is trademark infringement, but the cyber courts take cases concerning "online purchases of goods" and "online service agreements," which are more akin to contractual disputes. Moreover, a later judicial interpretation by SPC explicitly excludes contractual disputes arising from social media within the jurisdictional scope of cyber courts. The interpretation answers the question of "what is *not* subject to the cyber courts' jurisdiction," including an online purchase fulfilled via social media.[140] In other words, the cyber courts do not hear trademark infringement cases where plaintiffs bring claims only against social media platforms.

Without a viable option to hold online platforms secondarily liable for trademark infringement, brands have few options to identify the infringers and sue them directly. Currently, China has a real-name registration scheme, which requires Internet service providers to request and verify their users' real identity information.[141] However, real-name registration serves more for administrative purpose to regulate the cyberspace, placing heavier burdens on Internet service providers to monitor and report illegal content to the administration.[142] The cyber courts say nothing about indemnification for users' infringing conduct, and it is still up to the online platforms to use their discretion in revealing users' registration information.[143] Therefore, the establishment of cyber courts does not provide a valid cause of action for brands to enforce against online counterfeiters, and thus fails to provide the stronger enforcement mechanism that brands have long sought.

2. Issue Two: "Safe Harbor" for E-Commerce Platforms

China's E-Commerce Law is a similarly weak enforcement mechanism. The E-Commerce Law aims to crack down on the problem of online counterfeits by creating joint liability on e-commerce platform operators. But at the same time, the Law creates a "safe harbor" provision to balance the necessity of regulation and platforms' burden to monitor. With the safe harbor protection, platforms lack the incentive to cooperate with brands to enforce against infringers with stricter mechanisms.

The E-Commerce Law applies to three types of operators, e-commerce platform operators, third-party merchants, and online vendors.[144] The statute

---

140. Hu Shihao (胡仕浩), et al., <*Guanyu Hulianwang Fayuan Shenli Anjian Ruogan Wenti de Guiding*> *de Lijie yu Shiyong* (《关于互联网法院审理案件若干问题的规定》的理解与适用) [*Understanding and Applying the Provisions of the Supreme People's Court on Several Issues Concerning the Hearing of Cases by Internet Courts*], 28 PEOPLE'S JUDICATURE 24, 25 (2018).

141. Catherine Shu, *China Doubles Down on Real-Name Registration Laws, Forbidding Anonymous Online Posts*, TECHCRUNCH (Aug. 28, 2017, 1:07 AM), https://techcrunch.com/2017/08/27/china-doubles-down-on-real-name-registration-laws-forbidding-anonymous-online-posts/ [https://perma.cc/PLY8-D9V2].

142. *See id.* (indicating that the tech companies in China are pressured to serve as the government's gatekeepers).

143. *See supra* Part II.

144. Soo, *supra* note 126.

defines "e-commerce platform operators" as entities that "provide two or more parties to a transaction in e-commerce with services such as network business venues, deal-makings, and information distribution, for the two or more parties to the transaction to independently carry out business activities" (such as online shopping platforms like Amazon and Taobao).[145] A plain reading of the statute suggests that e-commerce platforms serve primarily for business transactions. The Law goes further by addressing the liability of the platforms in the case of IP infringement by third-party merchants. If platforms fail to take necessary methods, such as deleting, blocking links, or stopping transactions to the infringing merchants at trademark owners' notice, they are jointly liable for the infringing conduct by third-party merchants.[146] This provision creates a "safe harbor" for the e-commerce platform operators. Under Article 42 of the E-Commerce Law, if platforms have implemented a notice-and-takedown mechanism to respond to infringement reports and have performed accordingly, they are effectively immune from third-party action.

The concept of "safe harbor" originally comes from the copyright regime, which limits online service provider immunity from third-party users' infringing conduct.[147] In practice, many courts in China extend this theory to the trademark regime.[148] Some scholars point out that copyright and trademark protection share some common purposes and enforcement methods in the cyber world, but e-commerce platforms possess some distinctive features that suggest a heightened liability standard.[149] Many e-commerce platforms directly profit from the contractual relationship with third-party merchants by allowing them to list products and facilitate sales to customers, while in the context of copyright, most online services primarily provide storage or transmission of content.[150] In other words, trademark rights aim at preventing unfair competition and thus promoting a more robust market, which is distinct from copyright's purpose of encouraging creativity. So, the commercial nature of e-commerce platforms should deprive them of the safe harbor immunity given to other neutral online service providers.[151]

After all, current judicial practice does not inquire further into the question of whether the E-Commerce Law's "safe harbor" should be uniformly applied to all types of platforms. The "safe harbor" essentially leads brands back to the "whack-a-mole" situation. If platforms have fulfilled the obligation to delete, block, disconnect links, or end transactions or services to the alleged infringers upon notice, they are released from liability.[152] Thus,

145. E-Commerce Law, *supra* note 125, ch. II, sec. 1, art. 9.

146. *Id.* at ch. II, sec. 1, art. 45.

147. Yu Xiaoping (于晓萍), *Shilun Dianshang Wangluo Fuwu Pingtai de Jianjie Shangbiao Qinquan Guize—Jiantan Bifenggang Yuanze Zai Shangbiao Qinquan Zhong de Shiyong Wenti* (试论电商网络服务平台的间接商标侵权规制——兼谈避风港原则在商标侵权中的适用问题) [*Secondary Liability of E-Commerce Platforms—A Discussion of the Application of Safe Harbor Doctrine to Trademark Infringement*], 1 J. BEIJING C. POL. & L. 44, 46 (2018).

148. *Id.* at 47.

149. *Id.*

150. *Id.*

151. *Id.* at 49.

152. E-Commerce Law, *supra* note 125, ch. II, sec. 2, art. 42.

the E-Commerce Law does not give brands more leverage against platforms to impose greater obligations to assist with online trademark enforcement.

V. CHINA SHOULD AMEND ITS E-COMMERCE LAW TO IMPOSE THE JOINT LIABILITY REQUIREMENT ON SOCIAL MEDIA PLATFORMS THAT INCORPORATE IN-APP SHOPPING FEATURES.

Even though the establishment of the cyber courts and the implementation of the E-Commerce Law inadequately address the issue of online trademark enforcement, they provide some guidance for policing trademark on social media. Because the line between social media and e-commerce platforms is vanishing, there is a strong need for more powerful mechanisms to protect trademark owners' rights in response to the developing technology in the cyber world. This Note suggests amending China's current E-Commerce Law to classify social media platforms with in-app shopping features as e-commerce platforms. Along with the amendment, this Note also proposes other obligations, such as adopting a notice-and-takedown mechanism and a "three-strike" rule to deny access to repeat infringers on social media to better assist with trademark enforcement against counterfeiters.

In addition, the legal reform in China provides a lesson for the U.S. to strengthen trademark protection on e-commerce platforms. The cyber courts in China have been experimenting with blockchain for preserving and submitting digital evidence, which may improve litigation efficiency with regard to Internet-related disputes.

A. Amending China's E-Commerce Law

A key question is whether social media, especially those embedding in-app shopping features, fall within the definition of e-commerce platforms. Different business models on each social media platform may lead to different answers. For instance, WeChat's mini-programs spark a debate as to whether the platform should be liable for infringing behavior occurring on its sub-ports. Some practitioners argue that WeChat acts as a basic network service provider for mini-program developers.[153] It serves the developers with access and technical support to programming framework, and it is the developers who make and operate mini-programs on their own and engage in business activities.[154] In this sense, the mini-program developers, instead of WeChat,

153. Yang Yi (杨祎), *Weixin Dianshang Lei Xiaochengxu Kaifazhe Wei Pingtai Nei Jingyingzhe Weixin Ying Chengdan Pingtai Zeren* (微信电商类小程序开发者为平台内经营者 微信应承担平台责任) [*Mini-Programs Developers Are Intra-Platform Operators, and WeChat Should Undertake Platform Responsibility*], CHINA MKT. REG. NEWS (May 28, 2019), http://www.cicn.com.cn/zggsb/2019-05/28/cms117957article.shtml [https://perma.cc/6VFE-W5MP].

154. *See id.*

should be deemed "e-commerce platform operators." This line of argument analogizes the relationship between an app store and individual mobile applications.[155] Mini-programs function similarly as self-built websites or mobile applications that are spawned from a basic technological structure. They merely transfer the setup process from users' devices to WeChat's server, but all the other functions do not differ much from that of independent apps or programs.[156] Thus, the highly self-directed operation of mini-programs should strip contributory liability from WeChat as merely a technologically supportive platform.[157] A Hangzhou Intermediate People's Court[158] ruling supports this position, the first and only case concerning infringing conduct in a mini-program. In *Hangzhou Daodou Network Tech. Co. v. Changsha Baizan Network Tech. Co.*, the court ruled that WeChat only provided a basic access point to mini-program developers, and thus it should not be forced to delete the infringing materials, which were not even stored on WeChat's server.[159] Rather, it should provide adequate assistance for IP protection within its technological capability.[160]

Another view argues that mini-programs thrive because of how much users trust and accept WeChat.[161] WeChat's popularity provides a basis for mini-program developers to attract more users to their services, and this is why consumers tend to choose a mini-program in WeChat over other apps in an app store.[162] Therefore, WeChat has a closer relationship with these mini shops and should take responsibility. This argument probably applies more accurately to cases in which social media platforms do not use sub-ports, but instead operate their own in-app shopping malls on their servers. For example, Xiaohongshu's RED Mall functions similarly to other traditional e-commerce platforms, such as Taobao, where merchants come and open stores to engage in commerce with users. Such social media platforms deliberately set up a section to encourage in-app transactions and therefore behave more like e-commerce platform operators.

This second view is more compatible with the fact that social media platforms directly profit from the platform-merchant relationship.[163] Therefore, this Note suggests amending the current E-Commerce Law to

155. *See id.*

156. *See id.*

157. *See id.*

158. An intermediate people's court is the second lowest local people's court in China. It hears relevantly important cases on trial and appeal cases from primary people's courts, the lowest local courts.

159. Hangzhou Daodou Wangluo Keji Youxian Gongsi Su Changsha Baizan Wangluo Keji Youxian Gongsi, Shenzhenshi Tengxun Jisuanji Xitong Youxian Gongsi (杭州刀豆网络科技有限公司诉长沙百赞网络科技有限公司，深圳市腾讯计算机系统有限公司) [Hangzhou Daodou Network Tech. Co. v. Changsha Baizan Network Tech. Co. Ltd, Shenzhen Tencent Tech. Co.] (Hangzhou Interm. People's Ct. Nov. 5, 2019), at 15.

160. *Id.* at 15–16.

161. Yang, *supra* note 153.

162. *See id.*

163. *See, e.g.*, *Verification Service Fee*, Weixin Mini Program Verification Guidelines, WEIXIN GUANFANG WENDANG (微信官网文档) [WECHAT OFFICIAL DOCUMENTS] (last visited Sept. 13, 2020), https://developers.weixin.qq.com/miniprogram/en/product/renzheng.html [https://perma.cc/CX93-RGSC]; Constine, *supra* note 62.

recognize social media platforms embedding in-app shopping features as a variation of e-commerce platforms. Under the current law, many social media platforms linger in the grey area between communication service providers and commercial service providers. Because in-app shopping features promote greater user activity that in return benefits the social media platforms, the platforms should take more responsibility to regulate the e-commerce segments of their service. If such social media platforms are classified as e-commerce platforms, the notice-and-takedown system and joint liability for failing to take actions should also apply, thereby placing more obligations on social media to curb the problem of online counterfeits.

In addition, two other trademark protections should be implemented to supplement the amendment. First, some scholars suggest introducing a "three-strike" mechanism to impose a heightened standard on e-commerce platforms to monitor repeat infringers.[164] The E-Commerce Law requires platforms to establish a merchant verification archive as well as periodically update their verification system.[165] Platforms shall also record and store transactional information of the goods or services provided by merchants.[166] Under these provisions, platforms should have the capability to keep records of merchant information. If the platforms have received repeat infringement reports from a trademark owner against the same merchants, the platforms should be flagged and use their discretion to deny the infringers the ability to open any new stores.[167] Currently, some e-commerce platforms have their own "three-strike" rule, but whether the platforms enforce this rule and its effectiveness remain questionable.[168] Therefore, if a "three-strike" rule can be statutorily adopted, e-commerce platforms may have better incentive to strictly monitor repeat trademark infringers to avoid potential joint liability.

A second suggestion is to improve public information transparency on social media platforms. China's administration is exploring a viable approach in this direction. In February 2020, the Ministry of Commerce of the People's Republic of China ("MOC") issued a notice to solicit public comments on "Measures on the Management of E-Commerce Information Notices."[169] MOC proposed a draft regulation to supplement the E-Commerce Law to better protect the legal rights of consumers and IP rights holders.[170] The draft proposes a requirement for e-commerce platform operators to publicly disclose any decisions concerning intellectual property infringement on their platforms.[171] This approach is likely to help brands police their trademarks

164. Yu, *supra* note 147, at 50.

165. E-Commerce Law, *supra* note 125, ch. II, sec. 2, art. 27.

166. *Id.* at ch. II, sec. 2, art. 31.

167. *See* Yu, *supra* note 147, at 49.

168. *Id.* at 50.

169. *Guanyu <Dianzi Shangwu Xinxi Gongshi Guanli Banfa (Zhengqiu Yijian Gao)> Gongkai Zhengqiu Yijian de Tongzhi* (关于《电子商务信息公示管理办法（征求意见稿）》公开征求意见的通知) [*The Notice on Soliciting Public Opinions on the Administrative Measures on Electronic Commerce Information Publicity (Draft for Public Opinions)*], Ministry of Com. of People's Public of China (Feb. 12, 2020) (the draft is attached in http://tfs.mofcom.gov.cn/article/as/202002/20200202935276.shtml).

170. *Id.* at draft ch. 1, art. 1.

171. *Id.* at draft ch. 2, art. 21–24.

online and take worthwhile actions against specific counterfeiters. If the burden of keeping records of repeat trademark infringers shifts to the platforms, brands may selectively enforce against those that cause greater damages by continuing to sell counterfeits in different "mole holes."

Both supplementary protections—the "three-strike" mechanism and disclosure requirements—work better for trademark enforcement in the online context along with a recognition of social media platforms with in-app shopping features as e-commerce platforms. Because current e-commerce regulations provide brands with some viable enforcement mechanisms to patrol traditional e-commerce platforms, granting brands similar measures on social media may help enhance the protection of their trademarks.

B. China's Approach as a Lesson for the U.S. to Better Regulate the E-Commerce Market in Light of the SHOP SAFE Act.

Combating online counterfeits is not a China-exclusive challenge. Brands also seek powerful enforcement mechanisms on other mainstream social media platforms, as well as procedural support in litigation. By experimenting with cyber courts and blockchain-stored evidence, as well as adopting the E-Commerce Law, China's legal reform may provide some guidance for regulating online marketplace in light of recent efforts in the U.S. to propose the Stopping Harmful Offers on Platforms by Screening Against Fakes in E-Commerce (SHOP SAFE) Act.

In early March 2020, the U.S. House of Representatives introduced a bipartisan bill aimed at incentivizing e-commerce platforms "to adopt best practices designed to limit the sale of counterfeits that pose a risk to consumer health and safety."[172] The SHOP SAFE Act seeks to amend the Trademark Act of 1946 "to provide for contributory liability for certain electronic commerce platforms for use of a counterfeit mark by a third party on such platforms."[173] The bill uses vague language, leaving space to be filled up with more detailed definitions. For example, the bill defines "electronic commerce platform" as "any electronically accessed platform that includes publicly interactive features that allow for arranging the sale, purchase, payment, or shipping of goods, or that enables a person other than an operator of such platform to sell or offer to sell physical goods to consumers located in the United States."[174] This definition is too broad. Under a plain reading, any platforms that enable or facilitate in-app transaction would be considered e-commerce platforms.

The SHOP SAFE Act does not appear to designate social media as e-commerce platforms, and currently there is no example among U.S. social media that acts similarly as a shopping platform like WeChat or Xiaohongshu.

---

172. Press Releases, H. Comm. on the Judiciary, Nadler, Collins, Johnson & Roby Introduce Bipartisan SHOP SAFE Act to Protect Consumers and Businesses from the Sale of Dangerous Counterfeit Products Online (Mar. 2, 2020), https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=2838 [https://perma.cc/T5AJ-2LSE].

173. H.R. 6058, 116th Cong. pmbl., § 2 (2020).

174. *Id.* § 2.

Even though popular social media like Instagram and Snapchat venture their way into the e-commerce field, they only provide in-app transaction features to selective merchants or brands. Yes, when you scroll through the Instagram shop page or Facebook marketplace, you can see thousands of third-party postings selling knock-offs of luxury goods. But if you tap on those postings, the page will redirect you to an outside website, leading users away from the social media platforms. However, as more social media platforms become interested in exploring new possibilities to promote business activities within the app, China's experience in dealing with counterfeiters on social media may provide the U.S. with some insight.

Another groundbreaking legal development in China is worth mentioning to assist trademark litigation against online counterfeiters. China recognizes blockchain data as a legitimate method to preserve and submit electronic evidence. When addressing Internet-related disputes, courts have been concerned about the authenticity and integrity of electronic evidence, which affects its admissibility.[175] As e-commerce continues to thrive, lots of evidence, such as infringing postings, communication between merchants and users, and transactional records, are displayed and stored in an electronic format. Yet, online counterfeit listings are time sensitive because they are typically posted for only a few hours or days to avoid being monitored, which results in greater difficulty for timely tracking.[176] Besides, it is easier to alter or forge electronic evidence, which further burdens judges when determining its authenticity and integrity.[177] Without the ability to examine electronic evidence accurately, Chinese judges often rely on experts, which increases litigation costs.[178]

Blockchain technology may totally change the game in the field of electronic evidence. Blockchain's key features are irreversibility and incorruptibility.[179] Once a block of data is added to a ledger, it cannot be altered in any way, but can only be complemented with new blocks. The new blocks are added sequentially and time-stamped, creating a transparent view of the entire ledger history to preserve data integrity.[180]

In the context of online infringement, blockchain greatly improves the efficiency of disputed parties to preserve key evidence and jump the hurdle of evidence admissibility. In China, the traditional way to preserve electronic evidence is through notary agencies.[181] A valid notarization grants the authenticity of a piece of evidence, but the process is manual and takes a long

175. *See* Hong Wu & Guan Zheng, *Electronic Evidence in the Blockchain Era: New Rules on Authenticity and Integrity*, 36 COMPUT. L. & SEC. R. 1, 1 (2020).

176. Mostert, *supra* note 15, at 3.

177. Wu & Zheng, *supra* note 175, at 1.

178. *Id.* at 1–2.

179. *The Admissibility of Blockchain as Digital Evidence*, CONCORD L. SCH. (Apr. 23, 2019), https://www.concordlawschool.edu/blog/news/admissibility-blockchain-digital-evidence/ [https://perma.cc/2LZM-LGKU].

180. *Id.*

181. Zhou Qing (周庆) & Niu Ruifeng (牛瑞峰), *Qukuailian Canyu Wangluo Dianzi Zhengju Baoquan Gongzheng Chutan* (区块链参预网络电子证据保全公证初探) [*Preliminary Study on the Notarization of Online Electronic Evidence Preservation by Blockchain*], 40 J. HENAN INST. OF SCI. & TECH. 37, 39 (2020).

time.[182] In many cases, before a notary agency starts the preservation process, the relevant evidence may be lost or destroyed, leaving no ground for the notary agency to intervene.[183] If courts admit blockchain data, parties can upload electronic evidence by themselves to a designated system or server. They can also freely examine the evidence that has been stored with the courts and thus avoid potential damage to the original evidence.[184]

Chinese courts have set up a judicial blockchain system along with the establishment of the cyber courts.[185] The first court to adjudicate blockchain-facilitated electronic evidence was the Hangzhou Court of the Internet, which confirmed that electronic data stored on a blockchain could be admitted as electronic evidence.[186] Subsequently, in a 2019 case, *Huatai Yimei Ltd. v. Yangguang Feihua Ltd.*, that court admitted blockchain-generated evidence, which is different than evidence merely stored on blockchain, as authentic and integral.[187] The acknowledgement of blockchain data as evidence further serves China's goal of accelerating the adjudication process of Internet-related cases.

Several states in the U.S. have explored ways to implement blockchain technology in the field of evidence. In 2016, Vermont passed legislation declaring that "digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence."[188] Arizona and Ohio passed similar legislation acknowledging the "legal effect, validity or enforceability" of blockchain records.[189] It is foreseeable that additional states will start to consider the legal effect of blockchain-stored/generated data in courts in light of technological development and e-commerce progression. Therefore, China's judicial precedents provide U.S. practitioners with positive results in terms of embracing blockchain data for litigation purposes.

VI. CONCLUSION

In response to the drastic increase in the volume of e-commerce and the related increasing number of e-commerce-related lawsuits, China experiments with new methods to better regulate this area. The establishment of the cyber courts in China is a breakthrough virtually unmatched by any other country in the world. However, a mere simplification of procedures does not adequately help to break down the barrier to trademark enforcement in China. While China's enactment of the E-Commerce Law is a positive development in the fight against intellectual property infringement online, it

182. *Id.*
183. *Id.*
184. Li Jie (李杰), *Hulianwang Fayuan de Xianzhuang Yiji Qukuailian Cunzheng Quzheng Yanjiu* (互联网法院的现状以及区块链存证取证研究) [*Research on the Current Situation of the Cyber Courts and Evidence Preservation by Blockchain*], 29 J. SICHUAN VOCATIONAL & TECH. COLL. 13, 16 (2019).
185. Wu & Zheng, *supra* note 175, at 2.
186. *See id.*
187. *See id.*
188. VT H.868 (Act 157) (2018).
189. *The Admissibility of Blockchain as Digital Evidence*, *supra* note 179.

falls short in addressing trademark enforcement, especially on social media. Given that China thrives on international business transactions, including luxury goods, China should further improve its intellectual property regime by amending the E-Commerce Law and incentivizing social media to adopt stronger monitoring and enforcement methods to combat trademark infringement of global brands. Doing so would obtain trust and invite future collaboration and investment in the Chinese market.